ỦY BAN NHÂN DÂN TỈNH BÌNH DƯƠNG
TRƯỜNG CAO ĐẲNG NGHỀ VIỆT NAM - SINGAPORE

GIÁO TRÌNH

Mô đun: QUẢN TRỊ MẠNG 2

NGHỀ:QUẢN TRỊ MẠNG MÁY TÍNH

TRÌNH ĐỘ TRUNG CẤP NGHỀ

Ban hành kèm theo Quyết định số: /QĐ-TCĐNVS ngày tháng năm của Trường Cao đẳng nghề Việt Nam - Singapore

Bình Dương, năm 2017

LỜI GIỚI THIỆU

Qua thời gian giảng dạy tại trường Cao Đẳng nghề Việt Nam-Singapore cùng với các Thầy Cô trong khoa Công nghệ thông tin, bản thân tôi thấy cần biên soạn giáo trình về quản trị mạng 2 nhằm đáp ứng với chương trình giảng dạy hệ trung cấp nghề quản trị mạng máy tính. Nội dung của giáo trình được tham khảo và biên soạn theo tài liệu quản trị mạng máy tính của Microsoft và tài liệu quản trị mạng của Đại học khoa học tự nhiên thành phố Hồ Chí Minh. Giáo trình, trình bày về lý thuyết và các bước thực hành quản trị mạng máy tính, các giao thức truyền thông và các ứng dụng bao gồm những kiến thức cơ bản về các loại mạng, mô hình mạng, kiến trúc mạng, và các thiết bị kết nối mạng, mô hình OSI,TCP/IP … Với mong muốn tìm hiểu kỹ về công nghệ thông tin, mạng máy tính để có thể xây dựng, ứng dụng tối đa các tiện ích mà mạng máy tính mang lại sau khi học quản trị mạng 2 . Trong quá trình biên soạn giáo trình này dù đã cố gắng nhiều nhưng không thể tránh được những thiếu sót. Rất mong được sự góp ý của quí Thầy Cô để giáo trình này được hoàn chỉnh hơn.

Giáo trình này được biên soạn lại từ những nguồn tài liệu tham khảo khác nhau cho phù hợp với điều kiện giảng dạy tại Trường Cao đẳng nghề Việt Nam-Singapore và chỉ lưu hành nội bộ

Bình Dương, *ngày 31 tháng 12 năm 2018*

NGUYỄN ANH TUẤN- Tác giả

MỤC LỤC

GIÁO TRÌNH MÔ ĐUN 7
BÀI 1:DỊCH VỤ WINDOWS TERMINAL SERVICES 9
1.Các tính năng Terminal services 9
2.Mô hình xử lý của Terminal Services 10
2.1 Terminal Services kiến trúc 10
2.2 Giao diện điều khiển 10
3.Yêu cầu đối với Server của máy khách 10
4.Cài đặt, gỡ bỏ các phần mềm hổ trợ cho Terminal service 11
4.1Tạo các máy khách Terminal service 11
4.2 Điều chỉnh các thiết định của tài khoản kết nối 12
4.3Cấp phép sử dụng Terminal services 12
4.4 Quản lý các phiên làm việc của Terminal services 13
5. TÓM TẮT NỘI DUNG 23
6. CÂU HỎI VÀ BÀI TẬP 23
BÀI 2:TINH CHỈNH VÀ GIÁM SÁT MẠNG WINDOWS SERVER 26
1.Tổng quan về công cụ tinh chỉnh 26
1.1 Các nhật ký trong Event Viewer 26
1.2 Ứng dụng 26
1.3 Hệ thống 26
1.4 Bảo mật 26
2.Quan sát các đường biểu diễn hiệu năng bằng System Monitor 27
2.1 Tạo cách hiển thị hiệu quả nhất. 27
2.2 Lưu Bảng điều khiển System Monitor 27
2.3 Giám sát hiệu năng của máy chủ. 27
2.4 Giám sát hiệu năng bộ nhớ 27
2.5 Giám sát hiệu năng mạng 27
2.6 Giám sát các vai trò máy chủ 28
2.7 Sử dụng Performance Logs and Alerts 28
2.8. Tạo ra các counterlog (Nhật ký biến đếm): 28
2.9 Tạo các Alerts (Cảnh báo) 28
3.Giải quyết trục trặc bằng Event Viewer 29
3.1 Cấu hình nhật ký trong Event Viewer 29
3.2.Sử dụng các bộ lọc 29
3.3 Truy cập nhật ký sự kiện từ xa 30
3.4.Lưu giữ các Nhật ký sự kiện 30
4.Sử dụng Task Manager 30
4.1 Task Manager :(Trình Quản lý Tác vụ) 30
4.2 Giám sát các tiến trình 30
4.3 Giám sát mức hiệu năng 32
4.4 Giám sát các hoạt động của mạng 32
4.5 Giám sát người dùng 32
5.TÓM TẮT NỘI DUNG 39
6. CÂU HỎI VÀ BÀI TẬP 39

BÀI 3: KHÔI PHỤC SERVER KHI BỊ HỎNG 42
1.Các biện pháp phòng ngừa 42
2.Các phương pháp sao lưu dự phòng 42
2.1 Lưu đồ 42
2.2 Diễn giải lưu đồ 43
3.Tìm và quản trị Pan phần cứng bằng công cụ System Information 44
4.Giải quyết các trục trặc trong quá trình khởi động 45
5- TÓM TẮT NỘI DUNG 49
6. CÂU HỎI VÀ BÀI TẬP 50
Bài 4: CÀI ĐẶT VÀ QUẢN LÝ REMOTE ACCESS SERVICES (RAS) TRONG WINDOWS SERVER 52
1.Những ứng dụng thường gặp của RAS 52
2.Dự trù và những lưu ý về thông lượng đường truyền 52
3.Các yêu cầu về phần cứng để thực hiện RAS 52
3.1 Chuẩn bị 52
3.2 Đấu nối các thiết bị theo mô hình sau 53
4.Tiếp nhận các cuộc gọi từ người dùng ở xa 54
5.Kết nối một mạng VPN 55
5.1 Chuẩn bị 55
5.2 Cài đặt 55
5.3 Cấu hình 57
6.TÓM TẮT NỘI DUNG 58
7.CÂU HỎI VÀ BÀI TẬP 59
BÀI 5:GROUP POLICY OBJECT 61
1.Giới thiệu Group policy 61
2.Tạo và tổ chức các đối tượng trong Group policy 61
3.Thiết lập các chính sách trên Domain Controller 63
3.1 Xem chính sách cục bộ của một máy tính ở xa 63
3.2 Tạo các chính sách trên miền 64
3.3 Bài tập thực hành 64
4.Sử dụng GPO để triển khai Ms office 67
5- TÓM TẮT NỘI DUNG 74
6- CÂU HỎI VÀ BÀI TẬP 75
BÀI 6:GIỚI THIỆU VỀ ISA SERVER 79
1. Định nghĩa Firewall 79
2. Phân loại Firewall 79
2.1. Firewall phần mền 79
2.2. Firewall phần cứng 79
2.3. Bộ định tuyến không dây 79
3. Chức năng của Firewall 82
4. Các kiến trúc Firewall cơ bản 82
4.1. Tường lửa bộ lọc gói tin (Packet filtering firewall) 82
4.2. Cổng tần ứng dụng (Application gateway) 83
4.3. Bastion Host Firewall (Pháo đài phòng ngự). 84

5. Giới thiệu về ISA server....84
5.1.Điều Khiển Truy Nhập (Access Control)....84
5.2.Vị trí xảy ra quá trình xử lý gói....85
5.3.Luật lọc (Filtering Rules).....86
5.4 Hoạt động của tường lửa người đại diện ứng dụng (Proxy Application)....86
5.5.Quản lý xác thực (User Authentication)....86
5.6.Kiểm tra và Cảnh báo (Activity Logging and Alarms)....87
5.7.Các mô hình Firewall cơ bản và phức tạp....87
5.8.Sơ Đồ hoạt động của ISA....88
6.TÓM TẮT NỘI DUNG....89
7- CÂU HỎI....89
BÀI 7: CÀI ĐẶT VÀ CẤU HÌNH SỬ DỤNG CÁC RULE TRONG ISA....90
1.Cài đặt ISA....90
1.1 Chuẩn bị: Cài đặt ISA 2006 bản standart....90
1.2 Thực hiện....90
2.Tạo rule cho Admin đi ra ngoài Internet sử dụng tất cả các giao thức....91
3.Cấu hình cho các clien ra Internet chỉ sử dụng giao thức HTTP, HTTPS....92
4.Cấu hình DNS phân giải tên....94
5.TÓM TẮT NỘI DUNG....95
6.CÂU HỎI VÀ BÀI TẬP....96
BÀI 8:DỊCH VỤ VIRTUAL PRIVATE NETWORK....100
1.Giới thiệu về VPN....100
1.1.Bản chất hoạt động của VPN....100
1.2.Lợi ích của VPN....100
2.Mô hình VPN Client to Site dùng giao thức PPTP....101
3.Mô hình VPN Client to Site dùng giao thức L2TP/IPSec....104
4.Mô hình VPN Client to Site dùng chương trình No-IP....108
5.Mô hình VPN Site to Site....113
6.TÓM TẮT NỘI DUNG....115
7.CÂU HỎI VÀ BÀI TẬP....116
BÀI 9:PUBLISHING....118
1.Cài Đặt hệ thống Mail Mdaemon và gửi mail qua lại....118
2.Publishing Mail....120
3.Cấu hình Lọc mail....120
4.Publishing Web....121
5.Publishing FTP....122
6.Publishing Terminal Services....123
7.TÓM TẮT NỘI DUNG....135
8.CÂU HỎI VÀ BÀI TẬP....135
BÀI 10: MONITOR ISA SERVER....139
1.Trình bày các tab trong Monitor....139
1.1 Tab Session:....139
1.2 Tab Services:....139
1.3 Tab Report:....140

1.4 Tab Connectivity: 140
1.5 Tab logging: 141
2.Phát hiện các đợt tấn công gửi mail cho admin 141
3.Network Templates 144
4.Backup và Restore 145
4.1 Backup 145
4.2 Restore 146
5- TÓM TẮT NỘI DUNG 148
6- CÂU HỎI VÀ BÀI TẬP 149
CÁC THUẬT NGỮ CHUYÊN MÔN 151
TÀI LIỆU THAM KHẢO 153

GIÁO TRÌNH MÔ ĐUN

Tên mô đun: QUẢN TRỊ MẠNG 2

Mã số mô đun: MĐ 24

Thời gian thực hiện mô đun: 75 giờ; (Lý thuyết:30 giờ; Thực hành, thí nghiệm, thảo luận, bài tập: 42 giờ; Kiểm tra: 3 giờ)

I. Vị trí, tính chất của mô đun:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong các môn học chung, các môn cơ sở chuyên ngành đào tạo chuyên môn nghề bắt buộc.
- Tính chất: Là mô đun chuyên ngành bắt buộc.

II. Mục tiêu mô đun:

- Về kiến thức:
  + Có khả năng tinh chỉnh và giám sát mạng Windows Server;
  + Triển khai được dịch vụ Routing and Remote Access (RRAS);
  + Có khả năng phát hiện và khôi phục Server bị hỏng;
  + Có khả năng quản trị máy tính từ xa thông qua RAS;
  + Xây dựng được một mạng riêng ảo VPN;
  + Trình bày được các tính năng và những nét đặc trưng của ISA Server;
  + Trình bày được các cơ chế sao lưu, phục hồi toàn bộ máy ISA Server ;
- Về kỹ năng:
  + Cài đặt và cấu hình được ISA Server trên windows Server;
  + Xác định được các loại ISA Server Client đồng thời cài đặt và cấu hình đúng qui trình cho từng loại ISA Server Clien và những tính năng riêng trên mỗi loại.
  + Thực hiện cài đặt, cấu hình được các Rule theo yêu cầu;
  + Cài đặt và cấu hình được các chính sách mặc định của Firewall, thực hiện chính xác thao tác sao lưu cấu hình mặc định của Firewall;
  + Thực hiện cài đặt, cấu hình xuất, nhập các chính sách của Firewall ra thành file;
- Về năng lực tự chủ và trách nhiệm: Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập

III. Nội dung mô đun:

Số TT	Tên các bài trong mô đun	Thời gian			
		Tổng số	Lý thuyết	Thực hành	Kiểm Tra*
1	**Bài 1:**Dịch vụ Windows terminal services	5	3	2	
2	**Bài 2**:Tinh chỉnh và giám sát mạng Windows server	5	3	2	
3	**Bài 3:**Khôi phục server khi bị hỏng	5	2	2	1
4	**Bài 4**:Cài đặt và quản lý remote access services (RAS) trong Windows server	6	3	3	
5	**Bài 5**:Group Policy Object	11	4	6	1
6	**Bài 6**:Giới thiệu về ISA Server	4	4		
7	**Bài 7**:Cài Đặt và cấu hình sử dụng các Rule trong ISA	13	3	10	
8	**Bài 8**:Dịch vụ Virtual Private Network	11	3	8	
9	**Bài 9**:Publishing	13	3	9	1
10	**Bài 10**:Monitor ISA Server	7	2	5	
	Cộng	**75**	**30**	**42**	**3**

BÀI 1:DỊCH VỤ WINDOWS TERMINAL SERVICES

Mã bài:MĐ 24-01

Thời gian: 5 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày được các tính năng của Terminal Services
- Thực hành cài đặt và gỡ bỏ các phần mềm hổ trợ
- Tạo máy khách Terminal Services
- Quản lý được các dịch vụ của Terminal Services.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1.Các tính năng Terminal services

Terminal Service Remote Application là một tính năng mới trên Windows Server 2003. Các chương trình ứng dụng sẽ được cài đặt sẵn trên Windows Server 2003, các máy trạm tuy không cài đặt chương trình ứng dụng, nhưng vẫn có thể khai thác các chương trình ứng dụng đó trên máy chủ thông qua Terminal Service.

Terminal Services cung cấp khả năng lưu trữ nhiều phiên khách hàng đồng thời trên Microsoft Windows Server 2003. Terminal Server có khả năng lưu trữ trực tiếp các máy tính để bàn của khách hàng tương thích nhiều người sử dụng đang chạy trên một loạt các phần cứng trong Windows. Ứng dụng dựa trên chuẩn của Windows không cần sửa đổi để chạy trên máy chủ Terminal, và tất cả các tiêu chuẩn Windows Server 2003 dựa trên quản lý cơ sở hạ tầng và công nghệ có thể được sử dụng để quản lý các máy tính để bàn của khách hàng.

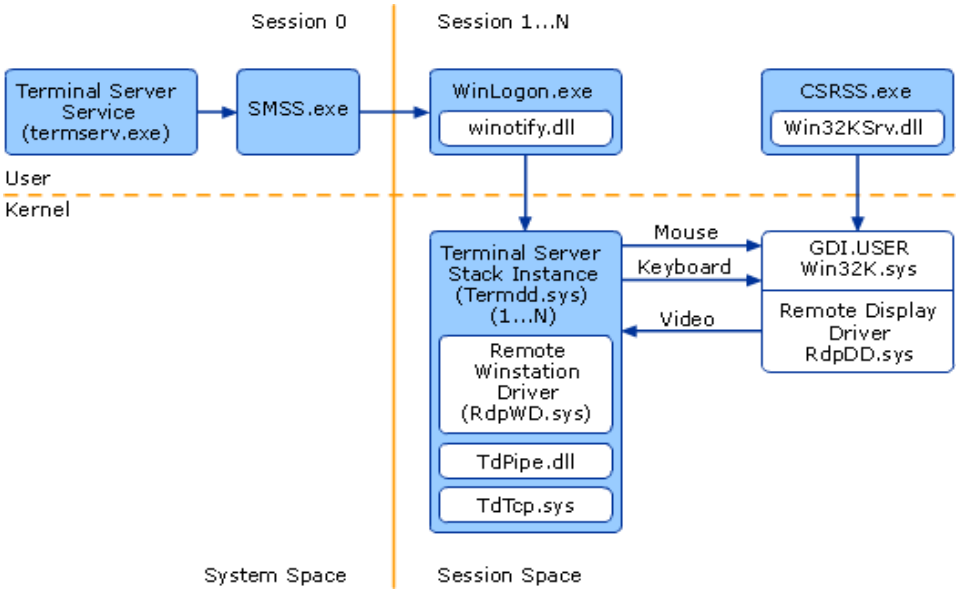
Remote Desktop khách hàng: phần mềm máy khách là một ứng dụng thiết lập và duy trì kết nối giữa khách hàng và máy tính một máy chủ đang chạy Terminal Services.

Terminal Services Licensing dịch vụ: Hệ thống này cho phép máy chủ đầu cuối quản lý thiết bị đầu cuối của khách hàng và cấp phép cho máy chủ truy cập (TS CAL) thẻ vào các thiết bị và người dùng kết nối đến một máy chủ đầu cuối.

Phiên dịch vụ Directory: Thư mục phiên (SD) giữ một danh sách các phiên được lập chỉ mục theo tên của người sử dụng, và cho phép một người dùng kết nối lại với máy chủ đầu.

2.Mô hình xử lý của Terminal Services

2.1 Terminal Services kiến trúc



Hình 1-1:mô hình kiến trúc Terminal Services

Khi Windows Server 2003 khởi động Terminal Server và tải hệ thống điều hành lõi, dịch vụ Terminal Server (termsrv.exe) được bắt đầu và bắt đầu chờ đợi cho các kết nối phiên. Mỗi kết nối là một định danh phiên độc đáo hoặc "sessionid" để đại diện cho một phiên làm việc cá nhân đến Terminal Server, và mỗi tiến trình được tạo ra trong một phiên "gắn thẻ" với sessionid liên quan đến sự khác biệt cho không gian tên của nó từ bất kỳ không gian tên phiên khác.

2.2 Giao diện điều khiển

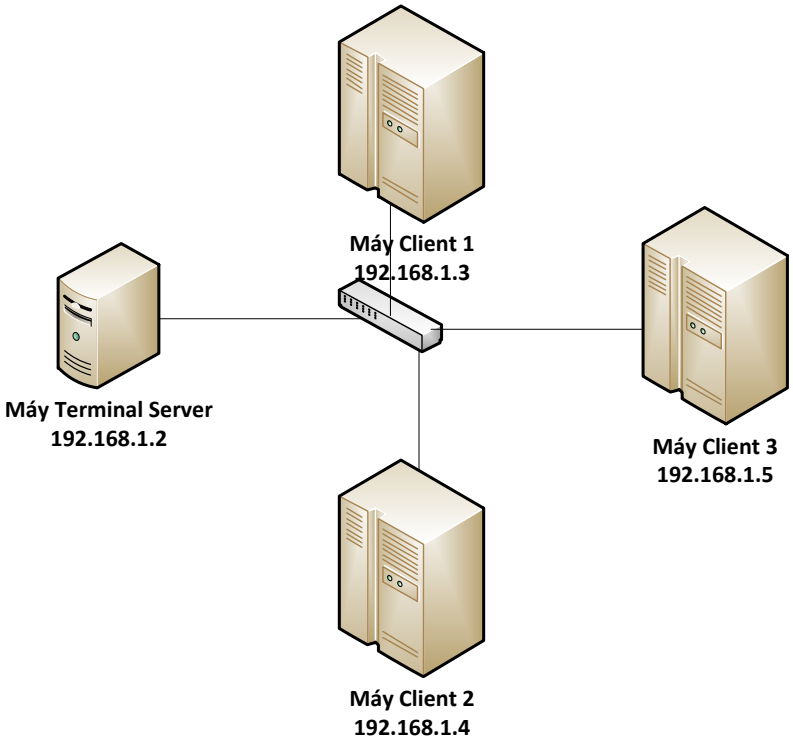
Giao diện điều khiển phiên họp (Terminal Server bàn phím, chuột, và video) luôn luôn là người đầu tiên để tải, được coi là một kết nối khách hàng đặc biệt, trường hợp được giao SessionID0. Giao diện điều khiển phiên họp bắt đầu như một phiên Windows Server 2003 bình thường, chuột Windows được cấu hình, màn hình hiển thị và trình điều khiển bàn phím được nạp.

Sau khi tạo giao diện điều khiển phiên họp, các dịch vụ Terminal Server sau đó gọi Session Manager Windows (SMSS.EXE) để tạo ra hai phiên nhàn rỗi của khách hàng, sau đó chờ đợi các kết nối khách hàng. Để tạo ra các phiên nhàn rỗi, Session Manager bắt đầu Client-Server Run-thời gian hệ thống con (Csrss.exe), và một sessionid mới được giao cho quá trình đó.

3.Yêu cầu đối với Server của máy khách

Giấy phép Terminal Server: Terminal Server Licensing là một dịch vụ thành phần của Windows Server 2003, Standard Edition, Windows Server 2003 Enterprise Edition và Windows Server 2003, Datacenter Edition. Nó có thể quản lý không có giấy phép, cấp giấy phép tạm thời, và khách hàng được cấp phép truy cập khách hàng, và hỗ trợ thiết bị đầu cuối máy chủ chạy Windows Server 2003. Điều này giúp đơn giản hóa các nhiệm vụ quản lý giấy phép cho người

quản trị hệ thống, trong khi giảm thiểu hoặc mua giấy phép cho một tổ chức. Thiết bị đầu cuối cấp phép Server chỉ được sử dụng với Terminal Server và không phải với Remote Desktop cho Quản trị.

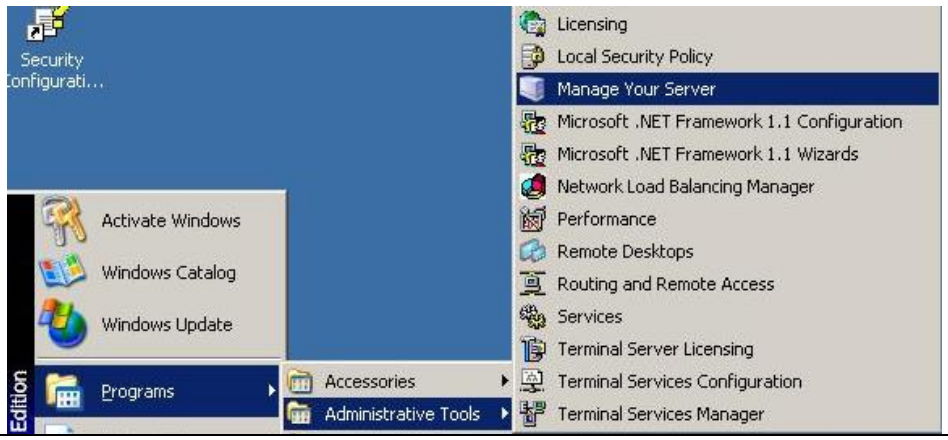


Hình 1-2:mô hình Terminal Server

4.Cài đặt, gỡ bỏ các phần mềm hổ trợ cho Terminal service

4.1Tạo các máy khách Terminal service

Bước 1:Vào Start → Programs → Administrative Tools → Manager Your Server

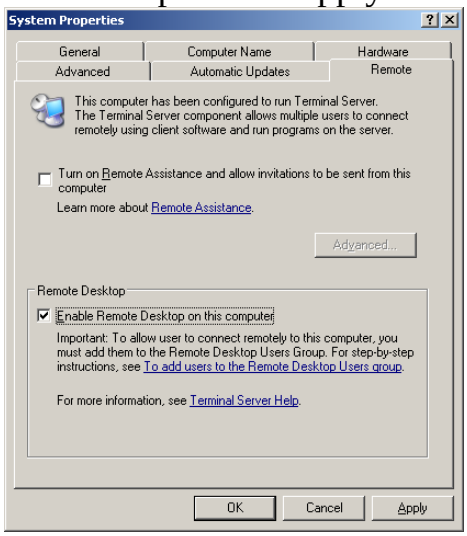


Bước 2: Click Add or remove a role→Next

Bước 3:Để mở chương trình quản lý Terminal Services Manager
Vào Start → Program → Administrative Tools → Terminal Services Manager

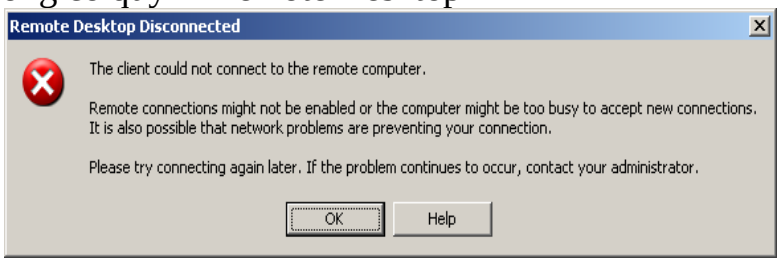
4.2 Điều chỉnh các thiết định của tài khoản kết nối

- Nếu khi kết nối đến máy tính cần Remote Desktop xuất hiện thông báo lỗi sau
- Click phải vào My Computer → Propertices → Tab Remote → Enable Remote Desktop on this computer → Apply → Ok


System Properties
General
Computer Name
Hardware
Advanced
Automatic Updates
Remote
This computer has been configured to run Terminal Server.
The Terminal Server component allows multiple users to connect remotely using client software and run programs on the server.
Turn on Remote Assistance and allow invitations to be sent from this computer
Learn more about Remote Assistance.
Advanced...
Remote Desktop
Enable Remote Desktop on this computer
Important: To allow user to connect remotely to this computer, you must add them to the Remote Desktop Users Group. For step-by-step instructions, see To add users to the Remote Desktop Users group.
For more information, see Terminal Server Help.
OK
Cancel
Apply

Hình 1-3: Tab Remote

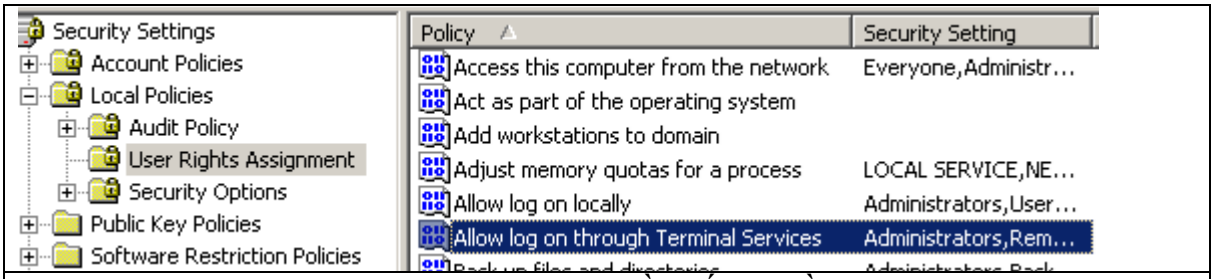
- Nếu khi thực hiện Remote Desktop mà xãy ra thông báo lỗi như bên dước là do chưa bật chức năng Enable Remote Desktop, hoặc do user đăng nhập không co quyền Remote Desktop


Remote Desktop Disconnected
The client could not connect to the remote computer.
Remote connections might not be enabled or the computer might be too busy to accept new connections. It is also possible that network problems are preventing your connection.
Please try connecting again later. If the problem continues to occur, contact your administrator.
OK
Help

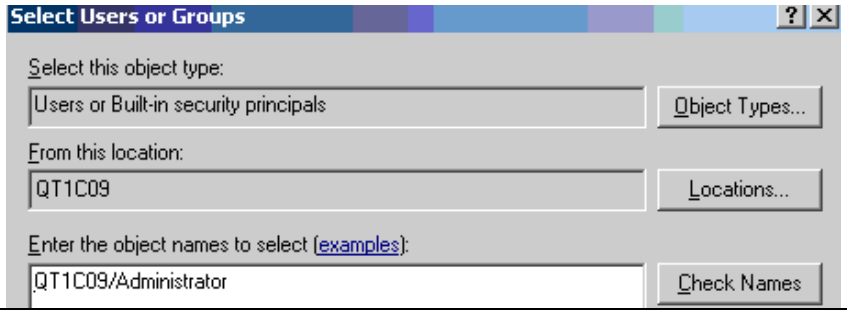
Hình 1-4: màn hình thông báo lỗi

4.3Cấp phép sử dụng Terminal services

Bước 1: vào Start → Program → Administrative Tools → Local Security Policy→ tìm đến khóa Allow log on through Terminal Services → R-Click → Propertices



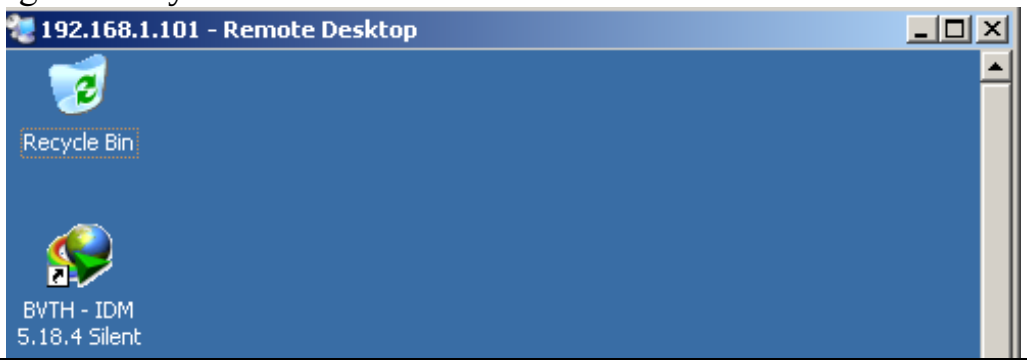
Bước 2: Add User or Group: nhập User cần cấp quyền truy cập dịch vụ → OK



4.4 Quản lý các phiên làm việc của Terminal services

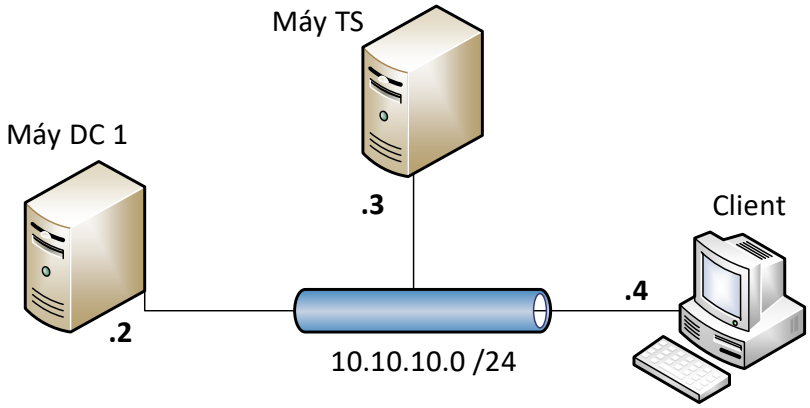
Bước 1: Start → Programs → Accessories → Communications → Remote Desktop Connection

Bước 2: Nếu trong Tab General không nhập username và password thì chương trình sẻ yêu cầu



Bài tập 1: thực hành

Cho mô hình mạng



Cấu hình Terminal Services trên Server 2008

Yêu cầu

- Nâng cấp máy DC1 lên domain controller
- Cấu hình Terminal services
- Gia nhập máy TS và máy Client vào Domain

Chuẩn bị

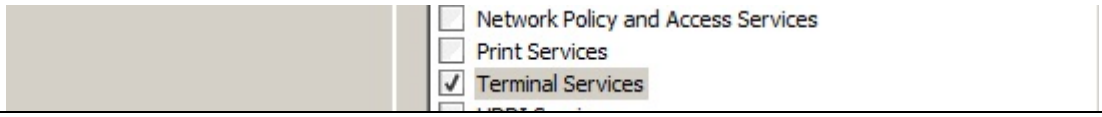
- máy cài win2k8
- 1 máy cài win7
- Tạo 2 user
- 1 user để truy cập terminal services VD: u1, pass: 123
- 1 user đề máy client đăng nhập: VD: client1 , pass 123

Thực hiện

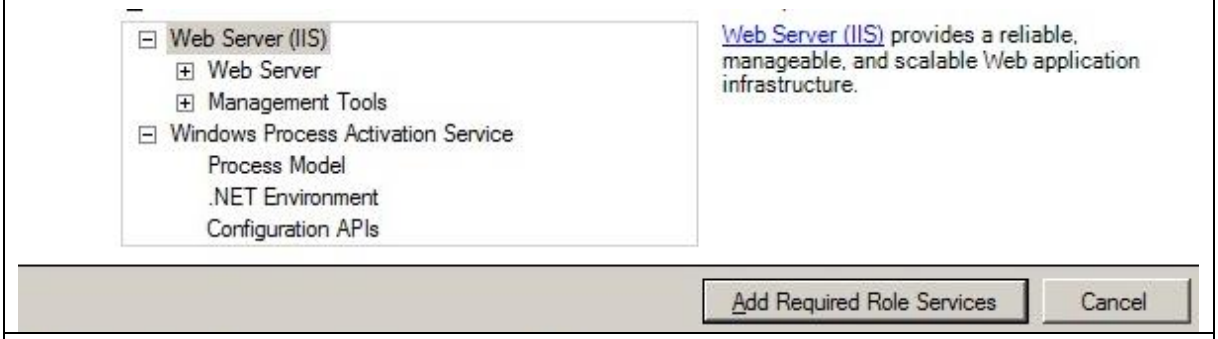
1.Cài đặt và cấu hình cho user truy cập đến máy terminal services bằng remote desktop connection

Bước 1: Cài đặt Terminal Service, trên máy TS → roles → Add Roles

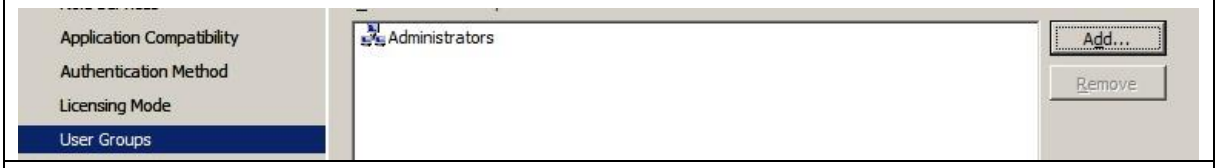
Bước 2: Chọn Next→ terminal Services → Next



Bước 3: Check chọn Terminal Services → TS Web Access→ Add …→ Next



Bước 4: Chọn Next→ Next→ Configuge later → Next Cấp quyền user truy cập→ chọn Add → thêm user "u1"



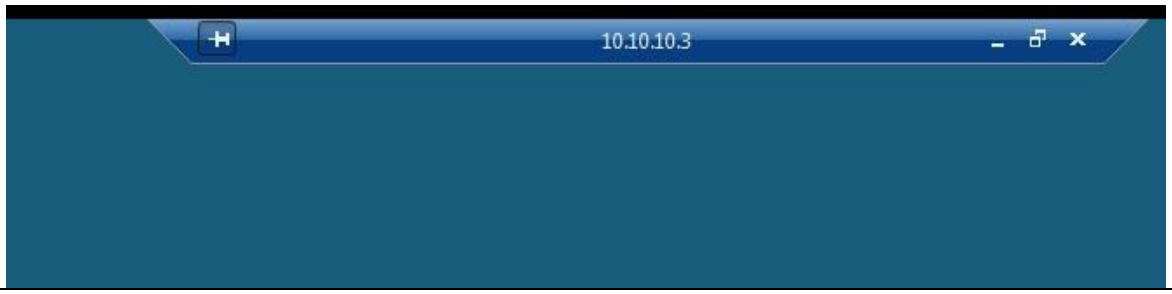
Bước 5: Sau khi thêm user → OK→ Next→ Next→ Next→ Chọn Install → sau đó khởi động lại máy

Authentication Method
Licensing Mode
User Groups
Web Server (IIS)
Role Services
Confirmation
Terminal Server
You may need to reinstall existing applications.
IE Enhanced Security Configuration will be turned off.
Authentication method: Do not require Network Level Authentication
Licensing mode: Configure licensing mode later
Groups allowed access: Administrators, u1 (u1@vsvc.com)
TS Web Access
Default TS Web Access site: http://TS/ts

Bước 6: Trên máy Client , đăng nhập bằng user "client1"; pass: 123 → start → program → accessries → remote desktop connection→ Option

Bước 7: Nhập IP: máy TS→ username: u1 đã tạo ban đầu

→Connect→password→yes



2.Cấu hình kết nối đến terminal Server thông qua TS Web Access

Bước 1: Thực hiện trên máy TS→truy cập đường dẫn: http://10.10.10.3/ts

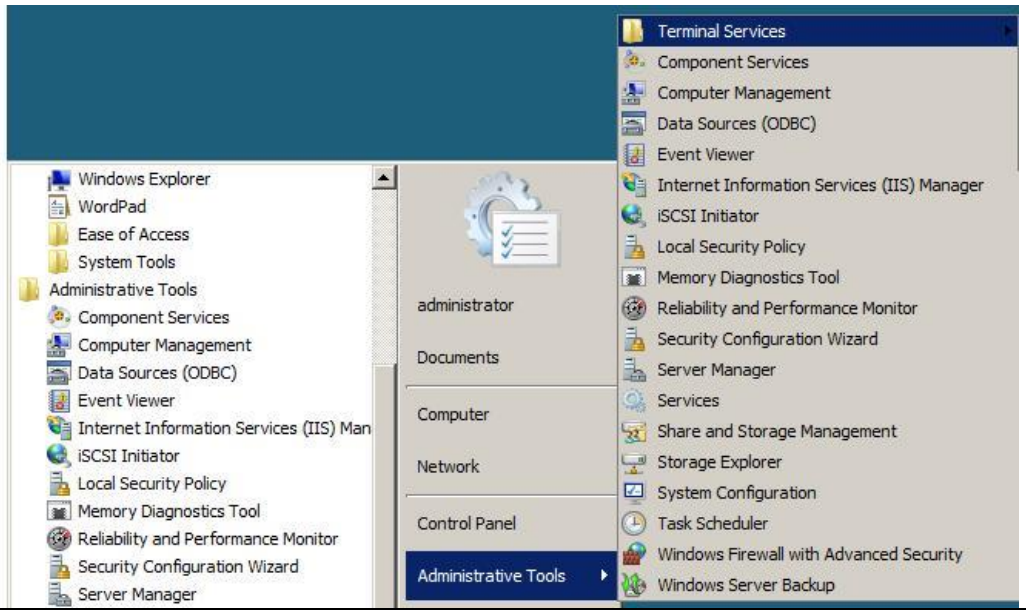
Nhập user "u1" đã tạo ban đầu

Bước 2: Click phải chuột Run Add-on→Run→ Tab Remote Desktop nhập IP máy TS → Connect

Windows Server® 2008
TS Web Access
RemoteApp Programs
Remote Desktop
Terminal Services Remote Desktop Web Connection
Enter the name of the remote computer that you want to connect to, specify options, and then click Connect.
Connection options
Connect to: 10.10.10.3
Remote desktop size: Full screen
Options >>
Connect

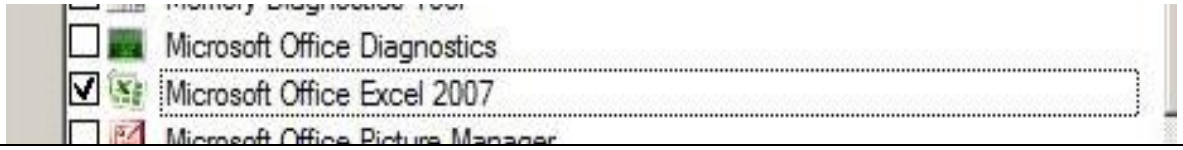
3.Cấu hình Remote Application

Bước 1: Thự hiện trên máy TS: cài đặt office 2007 ,vào start → Administrative Tolls → Terminal Services → TS RemoteApp Manager

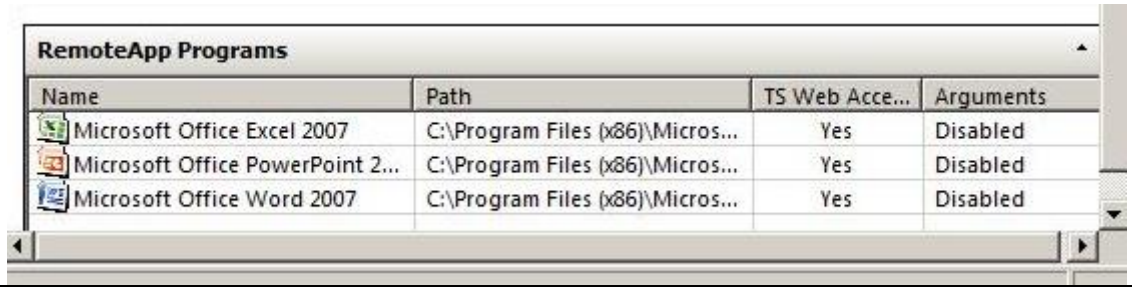


Bước 2: Chọn Action → Add RemoteApp Programs

Bước 3: Chọn Next→ word , excel, powerpoint →Next→ Finish



Bước 4: Tạo 3 file cài đặt



4.Cấu hình kết nối đến các ứng dụng tự xa thông qua Remote Application trên máy client mở trình duyệt. nhập http://10.10.10.3/ts

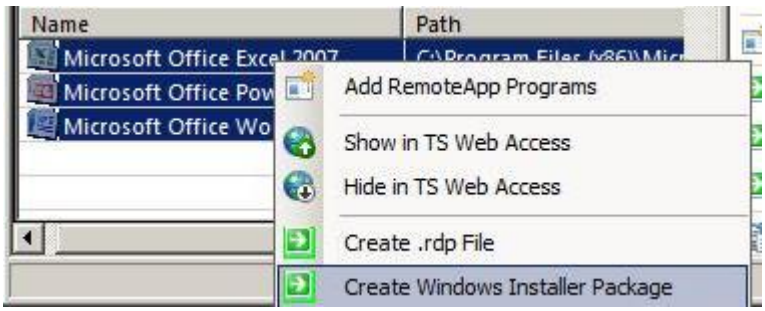
Bước 1: Nhập user name u1 và password→Remoteapp Programs → Word→ Connect

Đăng nhập u1→thành công

5.Tạo file MSI cho các ứng dụng Remote Application

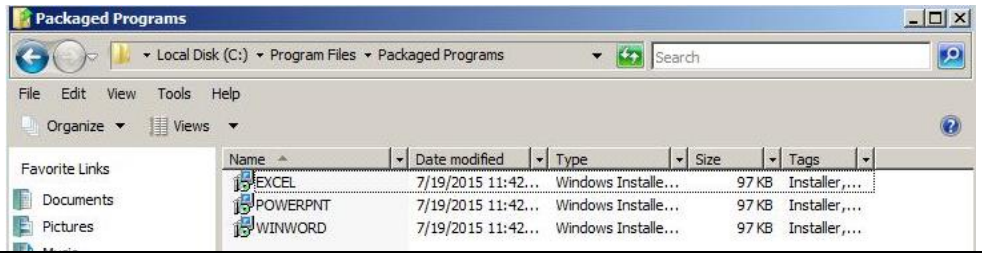
Thực hiện trên máy TS

Bước 1: Mở TS RemoteApp Manager vừa tạo ở trên → chọn 3file → click phải chuột Create windows install package→Next



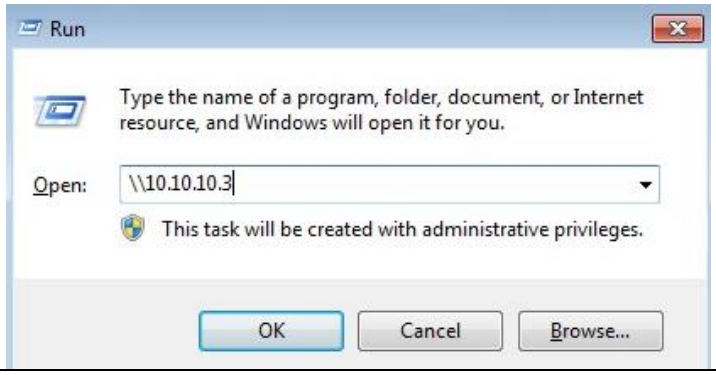
Chọn Next→ Next→ Next→ Finsh

Bước 2: Tạo 3 file .msi

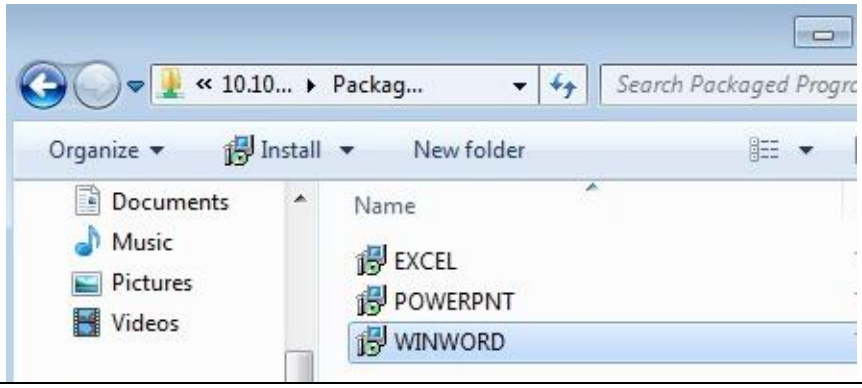


Bước 3: Share thư mục chứa 3 file vừa tạo

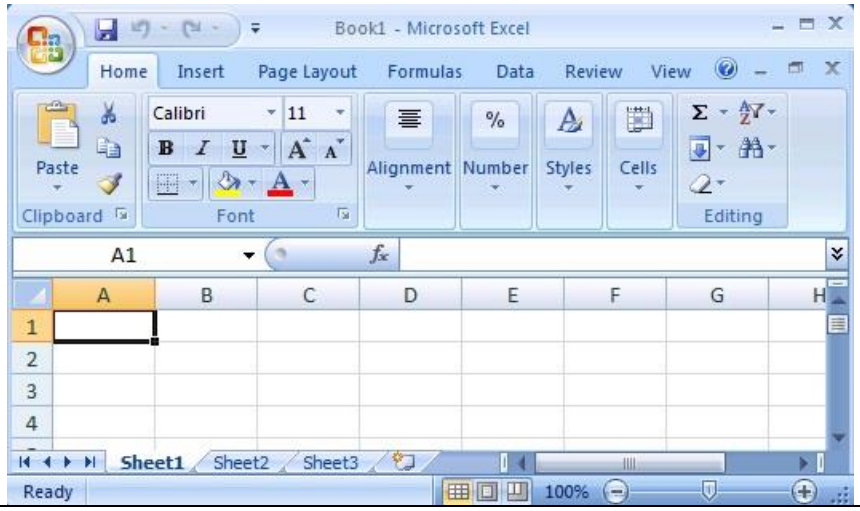
Bước 4: Trên máy client truy cập đến máy TS đường dẫn như sau:


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
\\10.10.10.3
This task will be created with administrative privileges.
OK
Cancel
Browse...

Bước 5: Chạy lần lượt 3 file



Bước 6: Sau khi cài xong 3 file trên vào start →remote programs chạy lần lượt 3 file→Chạy file excel trướcChọn Connect → u1 pass 123→Cài thành công



Bài tập 2 : Với sự tương tác của TS Web Access vào SharePoint Services nhằm mục đích đơn giản hóa trong vấn đề RemoteApp vào Server cho người sử dụng

Yêu cầu: Tích Hợp TS Web Access vào Windows SharePoint Services

Chuẩn bị:

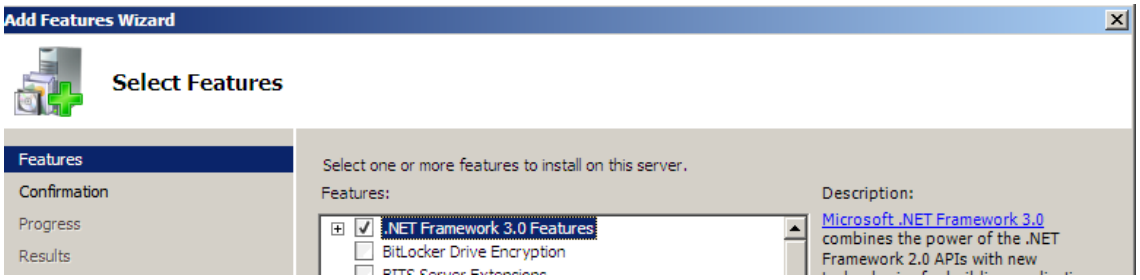
- Windows Server 2008
- Software: Sharepoint 3.0 SP1.

- Có thể Download tại:
    + Windows SharePoint Services 3.0 with SP1, 32-bit edition (http://go.microsoft.com/fwlink/?LinkId=106255)
    + Windows SharePoint Services 3.0 with SP1, 64-bit edition (http://go.microsoft.com/fwlink/?LinkId=106257)
      - Máy tính đã cài đặt và triển khai thành công TS Web Application

Thực hiện

1. Cài .Net Framework 3.0

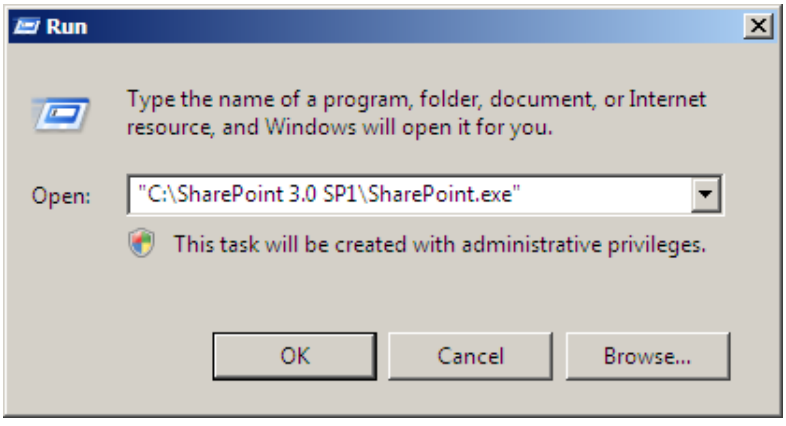
Bước 1: Mở Server Manager →Features →Add Features→ Select Features Check vào **.**Net Framework 3.0 Features →Next



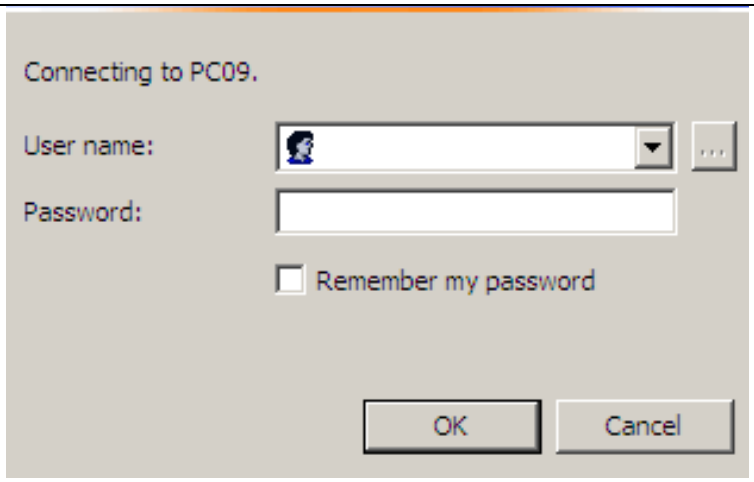
Bước 2: Chọn Install→ Quá trình cài đặt xong →Close

2. Cài SharePoint Service 3.0 SP1

Bước 1: Click Start → Run→Browse. Tìm đường dẫn đến files SharePoint.exe → Open→OK


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
"C:\SharePoint 3.0 SP1\SharePoint.exe"
This task will be created with administrative privileges.
OK
Cancel
Browse...

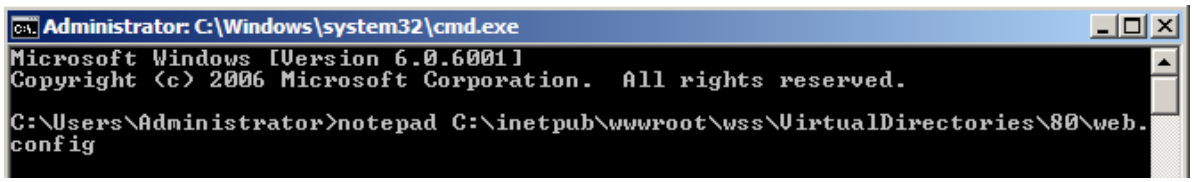
Bước 2: Xuất hiện cửa sổ Welcome to ... →Next→Yes→ Khi hệ thống Configuration đến 10 of 10 → Finish



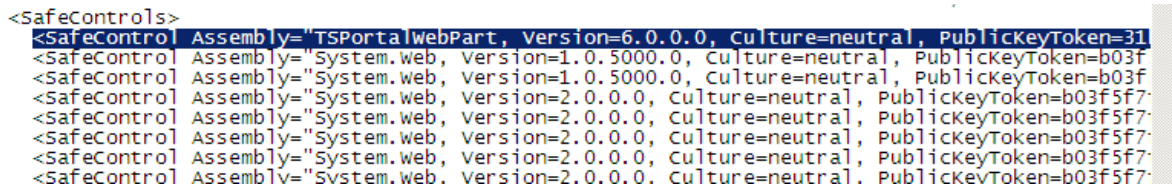
Xuất hiện cửa sổ đăng nhập vào trang quản lý SharePoint → Cancel. Và tắt Internet Explorer

3. Đăng kí Web Part's của TS Web vào SharePoint.

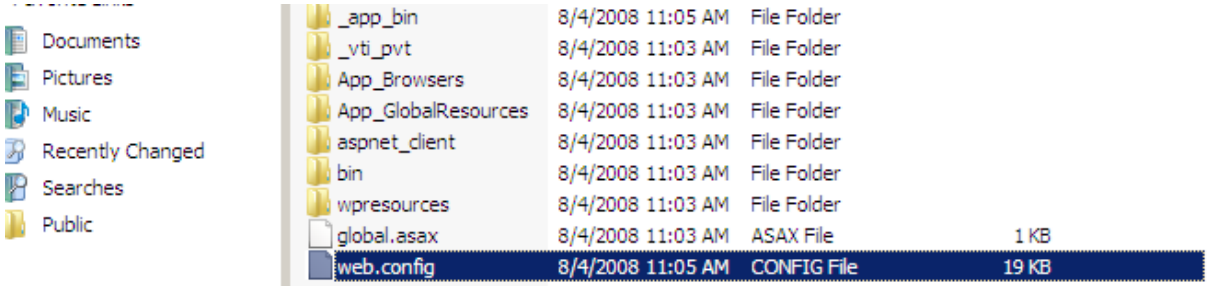
Bước 1: Vào CMD: gõ **notepad C:\inetpub\wwwroot\wss\ VirtualDirectories\80\web.config**


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>notepad C:\inetpub\wwwroot\wss\VirtualDirectories\80\web.config

Bước 2: Sau đó gõ dòng lệnh sau vào→ Save lại file web.config


<SafeControls>
<SafeControl Assembly="TSPortalWebPart, Version=6.0.0.0, Culture=neutral, PublicKeyToken=31
<SafeControl Assembly="System.Web, Version=1.0.5000.0, Culture=neutral, PublicKeyToken=b03f
<SafeControl Assembly="System.Web, Version=1.0.5000.0, Culture=neutral, PublicKeyToken=b03f
<SafeControl Assembly="System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7
<SafeControl Assembly="System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7
<SafeControl Assembly="System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7
<SafeControl Assembly="System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7

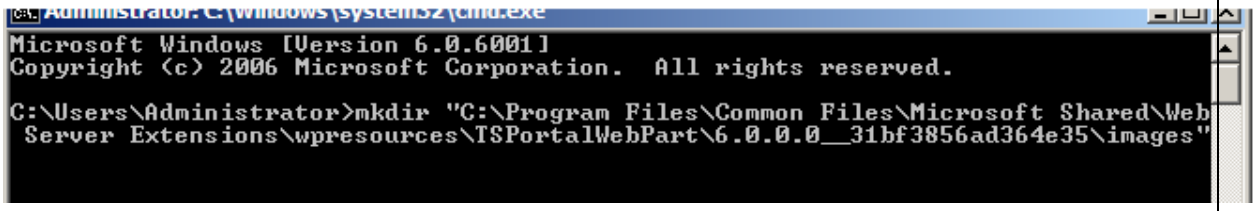
Bước 3: Vào C:\inetpub\wwwroot\wss \VirtualDirectories\port_number mở file web.config bằng Notepad


Documents
Pictures
Music
Recently Changed
Searches
Public
_app_bin 8/4/2008 11:05 AM File Folder
_vti_pvt 8/4/2008 11:03 AM File Folder
App_Browsers 8/4/2008 11:03 AM File Folder
App_GlobalResources 8/4/2008 11:03 AM File Folder
aspnet_client 8/4/2008 11:03 AM File Folder
bin 8/4/2008 11:03 AM File Folder
wpresources 8/4/2008 11:03 AM File Folder
global.asax 8/4/2008 11:03 AM ASAX File 1 KB
web.config 8/4/2008 11:05 AM CONFIG File 19 KB

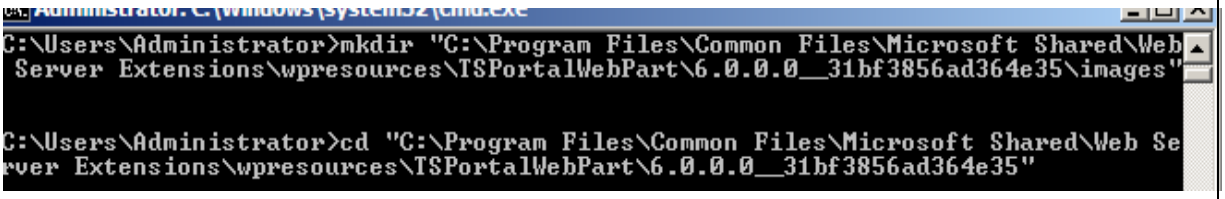
4. Tạo Web Part Image Files.

Bước 1: Vào CMD gõ: mkdir"C:\Program Files\Common Files \Microsoft Shared\Web Server Extensions\wpresources

\TSPortalWebPart\6.0.0.0__31bf3856ad36 4e35\images"


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>mkdir "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\wpresources\TSPortalWebPart\6.0.0.0__31bf3856ad364e35\images"

Bước 2: Gõ tiếp: icacls images /grant NetworkService:F

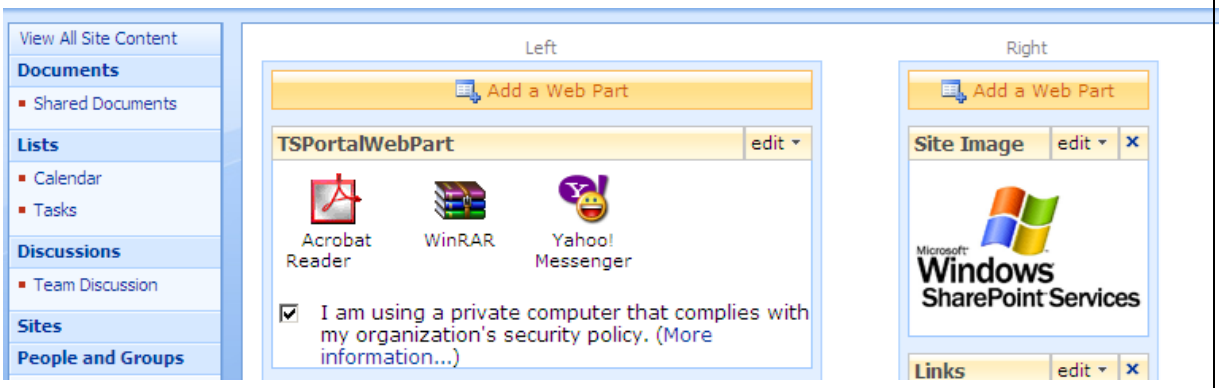

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>mkdir "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\wpresources\TSPortalWebPart\6.0.0.0__31bf3856ad364e35\images"
C:\Users\Administrator>cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\wpresources\TSPortalWebPart\6.0.0.0__31bf3856ad364e35"

5. Đưa TS Web Access vào SharePoint.

Bước 1: Mở IE truy cập: **http://localhost** → Xuất hiện cửa sổ đăng nhập : User name: administrator / pasword: 123

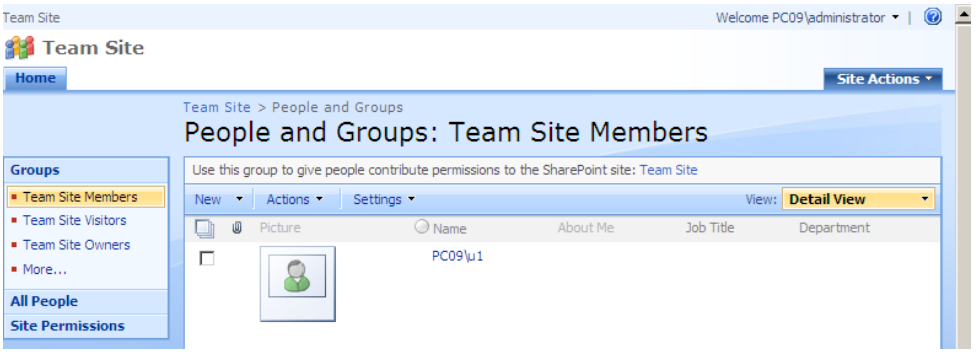
Bước 2: Chọn Add→ Close→ Chọn Site Actions → Site Settings

Bước 3: Tìm TSPortalWebPart check vào → TSPortalWebPart.webpart với những Application trong TS Web Access lúc ban đầu.



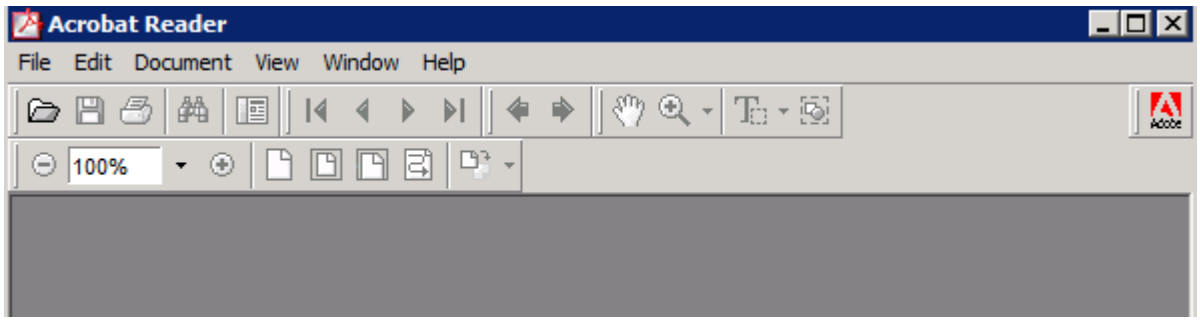
6. U1 RemoteApp vào TS Web Server thông qua SharePoint.

Bước 1: vào People and Groups → New→ Add Users → nhập u1 Check→OK→



Bước 2: Logon U1: Mở IE gõ http://locahost. Đăng nhập User name: u1 / pasword:123→**:** Mở Acrobat Reader→ Connect

→ Khai báo Password



5. TÓM TẮT NỘI DUNG

- Terminal Service RemoteApp đó chính là sự truy cập ứng dụng đường liền mạch đối với người dùng.
- Dễ dàng quản lý các văn phòng chính
- Terminal Service RemoteApp sử dụng tài nguyên máy chủ tốt hơn
- Terminal Service RemoteApp cho phép người dùng try cập hosting mọi nơi với đủ các thành phần thiết kế. Người dùng có thể truy cập trên máy tính laptop, mày tính để bàn.

6. CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1:Tại sao phải dùng Terminal services?

Câu 2:Hãy giới thiệu và trình bày đặc điểm Terminal services 2008

Câu 3: Trình bày các hình thức máy trạm kết nối đến máy chủ trong Terminal services 2008

BÀI TẬP

Bài tập 1:: Terminal server dùng chế độ mã hóa native RDP . Chế độ này không chứng thực server . Do đó để gia tăng tính bảo mật khi remote desktop thì chúng ta sẽ sử dụng Transport Layer Security (TLS) version 1.0 . Với chế độ này chúng ta có thể mã hóa và chứng thực máy remote tới server gia tăng độ bảo mật khi Remote Desktop bằng SSL .

Yêu cầu:.Cài đặt, cấu hình Transport Layer Security (TLS)

Chuẩn bị

- Máy client cài windows XP và cài RDP 5.2. Máy Terminal server cài windows server 2003 SP1 trở lên cài các component sau : (cài theo thứ tự)

1. ASP.net
2. IIS

3. Stand alone – CA

Hướng dẫn làm bài

1. Cấu hình trên máy Terminal Server

Cài đặt Certificate

B1 : Mở Internet explorer : đánh vào địa chỉ **http://IP_máy_server/certsrv**

B2 : Chọn Request a certificate

B3 : Chọn Advanced Certificate Request

B4: Chọn Create and submite a request to this CA

B5 : Điền thông tin trong phần **Identifying Information**

B6 : Start → Program → Administrative tools → Certification Authority → Chọn Pending Request

B7 : Chuột phải lên CA trong đây → All tasks → Issue

B8 : Mở IE → truy cập http://IP_máy_server/certsrv

2.Cấu hình Transport Layer Security : chứng thực và mã hóa

B1 : Start → Program → Administrative tools → Terminal Services Configuration

B2 : Trong khung bên trái chọn connection → Khung bên phải : chuột phải RDP-tcp → chọn Properties

B3 : Trong tab General → Chọn Edit

B4 : Chọn CA đã xin → Ok→ OK

B5 : Trong phần security layer có 3 lựa chọn : dùng chế độ SSl

3. Download CA từ máy Server và import vào client

a.Thực hiện trên Server

B1 : Mở IE đánh địa chỉ : http://localhost/certsrv

B2 : Chọn Download a CA certificate , certificate chain , or CLS

B3 : Chọn Download a certificate

B4 : Chọn Save → chọn nơi lưu → copy file mới save vào USB để dành

b.Thực hiện trên client :

B1 : Mở start → run → đánh lệnh MMC

B2 : Menu File → Chọn add/remove spap-in → chọn Add

B3 :Chọn Certificates

B4 : Chọn Computer accounts → next >→Finish

B5 : Chỉnh Regedit → Start → run → regedit → tìm đến khóa HKEY_LOCAL_MACHINE\SOFTWARE→Microsoft→Terminal Server Client

B6: Chuột phải lên Terminal Server Client → chọn New → Dword value → Sửa tên giá trị mới tạo thành AuthenticationLevelOverride

B7: Double click vào AuthenticationLevelOverride → Trong ô value data đánh vào gía trị : 1

B8 : Kiểm tra : Start → program → remote desktop connection

B9 : Trong cửa sổ remote connection → chọn option →qua tab security → Quan sát trong mục Authentication → là Required Authentication

B10: Qua tab General →điền vào phần computer cái tên CA mà bạn đã xin trên server

B11 : Remote thành công → quan sát thấy đường truyền giữa client và server đã được mã hóa

Bài tập 2: **Remote Desktop Service trên windows server 2012**

Yêu cầu: Cấu hình cấp phép RMS đến win server 2012

Chuẩn bị:

- 1 máy PC cài win2012 làm DC
- 1 máy PC cài win2012 làm computer member domain
- Hệ thống gồm có các server và client

Hướng dẫn làm bài

B1: Trên Server→run→sysdm.cpl →tab Remote.

B2:Mặc định hệ thống không cho phép các kết nối từ xa.Ta chọn Allow remote connections to this computer

B3: Chọn Select user để add user ta muốn cho remote vào server

B4: Domain Controller: mặc định không có đối tượng nào được remote (kể cả admin, muốn cho remote phải vào chỉnh Policy (1) trong Default Domain Controller Policy)

B5:Đăng nhập rồi: run → mstsc (remote desktop connection), điền thông tin user, password

BÀI 2:TINH CHỈNH VÀ GIÁM SÁT MẠNG WINDOWS SERVER

Mã bài:MĐ 24-02

Thời gian: 5 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày được chức năng của Mornitoring server performance
- Giải quyết được các sự cố mạng thông qua Event Viewer
- Kiểm tra được tần suất hoạt động của hệ thống tại từng thời điểm khác nhau Task Manager.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1.Tổng quan về công cụ tinh chỉnh

Mornitoring server performance :Là những chương trình giúp người quản lý thu thập được các thông tin về hiệu năng của server để họ có thể đảm bảo các server chạy tối ưu, hiệu quả và đáng tin cậy.

Nhiệm vụ chính: giám sát hiệu năng làm việc của server

1.1 Các nhật ký trong Event Viewer

Khi nạp ứng dụng Event Viewer, khung Phạm vi chứa một danh sách các nhật ký duy trì trong hệ thống.

1.2 Ứng dụng

Chứa các thông tin về các chương trình chạy trong máy tính, được xác định bởi các nhà phát triển ứng dụng

1.3 Hệ thống

Chứa các thông tin về các sự kiện do các cấu thành của Windows Server 2003 sinh ra. Ví dụ: như các dịch vụ hoặc trình điều khiển thiết bị. Một dịch vụ không khởi động được hoặc một trình điều khiển không thể nạp trong quá trình khởi động hệ thống sẽ được ghi lại trong nhật ký Hệ thống. Các kiểu sự kiện ghi được trong nhật ký này được hệ điều hành cấu hình trước và không thể thay đổi được.

1.4 Bảo mật

Có thể chứa các thông tin về các sự kiện liên quan đến bảo mật, ví dụ như không đăng nhập thành công, các truy cập đến các tài nguyên được bảo vệ (Ví dụ như các thư mục chia sẻ hoặc file hệ thống) và sự thành công hoặc thất bại của các sự kiện được kiểm định (audit). Windows Server 2003, trong cấu hình mặc định của nó, không ghi thông tin trong nhật ký Bảo mật. Các sự kiện ghi lại trong nhật ký này được xác định bởi các chính sách kiểm định có thể kích hoạt bằng các chính sách Cục bộ của Máy tính (Local Computer Policy) hoặc các Chính sách Nhóm (Group Policy). Theo mặc định, chỉ có các thành viên của nhóm Administrators mới có khả năng xem các nhật ký này

2.Quan sát các đường biểu diễn hiệu năng bằng System Monitor

2.1 Tạo cách hiển thị hiệu quả nhất.

Chỉnh sửa thuộc tính hiển thị của biến đếm. Tùy thuộc vào kích thước và khả năng của màn hình, màu mặc định và độ rộng của các đường sử dụng trong đồ thị của System Monitor có thể gây khó khăn khi phân biệt các biến đếm. Trong thẻ Data của hộp thoại System Monitor Properties của mỗi biến đếm, có thể chỉnh sửa màu sắc, kiểu và độ rộng của đường thể hiện biến đếm đó trong đồ thị để dễ dàng phân biệt với các biến đếm khác.

2.2 Lưu Bảng điều khiển System Monitor

Để có thể lưu lại như một file bằng cách chọn Save as từ thực đơn File và chỉ ra tên của file với phần mở rộng .msc. Nạp bảng điều khiển từ file này sẽ mở Performance console và hiển thị snap-in System Monitor, với tất cả các biến đếm và các thuộc tính hiển thị đã cấu hình trước khi lưu nó lại.

2.3 Giám sát hiệu năng của máy chủ.

Phương pháp thực hành tốt nhất là tạo ra một chiến lược giám sát máy chủ ngay sau khi máy chủ này được cài đặt và cấu hình đầy đủ. Theo cách này, có thể thiết lập một đường cơ sở hiệu năng (baseline) cho máy chủ trong các trạng thái hiệu năng lúc sử dụng thông thường, lúc nghỉ và lúc làm việc tại mức đỉnh. Khi có sự cố xảy ra trong các lần giám sát sau đó, việc đo lại lần nữa giá trị đường cơ sở này có thể giúp tìm ra giải pháp cho việc giải quyết sự cố.

2.4 Giám sát hiệu năng bộ nhớ

Một bộ nhớ không đủ cho máy chủ thường xuyên các dữ liệu cần thiết, gây ra việc các tiến trình phải dựa vào việc đọc đĩa hơn là đọc bộ nhớ và do đó làm giảm tốc độ của toàn hệ thống. Bộ nhớ là một phân hệ đơn quan trọng nhất cần phải giám sát bởi vì các sự cố trong bộ nhớ có thể ảnh hưởng đến tất cả các phân hệ khác.

2.5 Giám sát hiệu năng mạng

Network Interface: Bytes Total/sec (Giao tiếp mạng:Tổng số Byte/giây). Cho biết số lượng byte gửi và nhận trên giây trên một giao tiếp mạng.

Network Interface: Output Queue Length (Giao tiếp mạng:Độ dài hàng đợi ra). Cho biết số lượng gói tin đợi để truyền đi qua giao tiếp mạng

Server: Bytes Total/Sec (Máy chủ: Tổng số byte/giây). Cho biết tổng số byte gửi và nhận bởi máy chủ trên tất cả các giao tiếp mạng của nó.

Tăng tốc độ của mạng. Điều này có nghĩa là thay thế tất cả các giao tiếp mạng trong mọi máy tính, hub, router và các thiết bị khác trên mạng và có thể thay thế cả cáp mạng.

2.6 Giám sát các vai trò máy chủ

Khi giám sát hiệu năng máy chủ và tìm kiếm các nghẽn cổ chai, điều quan trọng là phải hiểu sự liên quan của các vai trò mà máy chủ đó thực thi. Các ứng dụng và dịch vụ có các yêu cầu khác nhau đến tài nguyên hệ thống và chính sách giám sát cho mỗi máy chủ nên tập trung vào các đối tượng cần đo hiệu năng và các biến đếm hiệu năng của các tài nguyên ảnh hưởng lớn nhất đến máy chủ đó.

2.7 Sử dụng Performance Logs and Alerts

Counter Logs (Nhật ký các biến đếm). Cho phép Performance console chụp các thông số thống kê cho các biến đếm nhất định vào một file nhật ký tại các thời điểm xác định và đều đặn sau một khoảng thời gian cố định

Trace Logs (Nhật ký theo dõi). Cho phép Performance console ghi lại các thông tin về các ứng dụng hệ thống khi một sự kiện nào đó xảy ra.

Alerts (Cảnh báo). Cho phép Performance console giám sát giá trị của một biến đếm nhất định nào đó theo các khoảng thời gian lặp và thực hiện một hành động xác định khi biến đếm đó đạt đến giá trị giới hạn nào đó.

2.8. Tạo ra các counterlog (Nhật ký biến đếm):

Các Performance objects và Performance counters. Chọn các performance objects và Performance counters và cả giao diện giống như khi sử dụng System Monitor.

Sample Interval (Thời gian lặp lấy mẫu). Thời gian lặp mà tại đó snap-in này sẽ ghi vào nhật ký giá trị của biến đếm đã lựa chọn. Lưu ý rằng thời gian lặp lấy mẫu mà ngắn sẽ cho ra file nhật ký lớn và đồng thời hệ thống sẽ phải làm việc nhiều hơn.

Run as credentials (Các thông số đăng nhập Run as). Tên người dùng và mật khẩu mà dịch vụ Performance Logs and Alerts sử dụng để đăng nhập vào hệ thống trước khi chụp các thông tin vào trong nhật ký biến đếm.

Log file type (Kiểu file nhật ký). Định dạng file nhật ký muốn sử dụng cho nhật ký biến đếm và thư mục muốn lưu.

2.9 Tạo các Alerts (Cảnh báo)

Counters (biến đếm). Các performance object và các performance counter có thể lựa chọn để cảnh báo, và giao diện sử dụng để lựa chọn chúng giống như trong System Monitor

Giá trị giới hạn của biến đếm. Đối với mỗi biến đếm lựa chọn, phải chỉ ra một giá trị giới hạn và muốn cảnh báo này sẽ được kích hoạt khi giá trị của biến đếm này thấp hơn hay cao hơn giới hạn.

Quãng ngắt lấy mẫu. Thời gian lặp mà theo đó snap-in sẽ thu thập giá trị của biến đếm lựa chọn

Các thông số đăng nhập Run as. Tên người dùng và mật khẩu mà dịch vụ Performance Logs and Alerts sử dụng để đăng nhập vào hệ thống trước khi giám sát các biến đếm được lựa chọn.

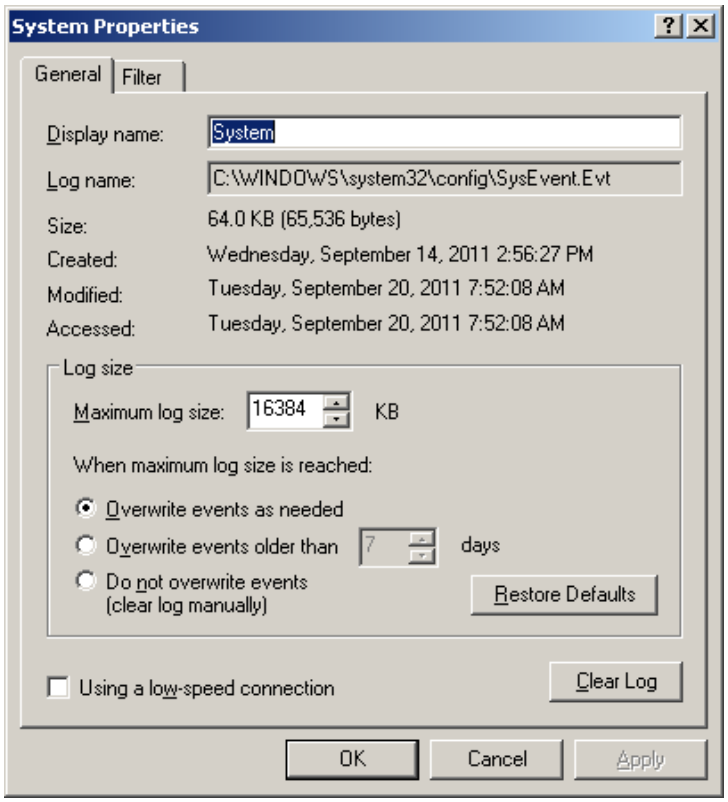
Hành động (Action). Hành động muốn snap-in thực hiện khi một trong các biến đếm lựa chọn đạt đến giá trị giới hạn. Snap-in có thể tạo ra một mục trong nhật ký sự kiện, gửi một thông báo qua mạng đến người dùng xác định nào đó, bắt đầu ghi các dữ liệu.

3.Giải quyết trục trặc bằng Event Viewer

3.1 Cấu hình nhật ký trong Event Viewer

Các lựa chọn duy trì nhật ký :

+ Overwrite Events As Needed (Ghi đè các sự kiện khi cần):
+ Overwrite Events Older Than X Days (Ghi đè sự kiện cũ hơn X ngày): Nhật ký sẽ duy trì các mục trong một số ngày (1 đến 365) xác định bởi lựa chọn này và ghi đè các mục cũ hơn nếu cần.
+ Do Not Overwrite Events (Clear Log Manually) (Không ghi đè nhật ký (Xóa nhật ký thủ công)): Hệ thống duy trì mọi mục của nhật ký cho tới khi chúng được xóa đi một cách thủ công bởi người quản trị.



Hình 2-1:màn hình nhật ký sự kiện

3.2.Sử dụng các bộ lọc

Để triển khai một bộ lọc trên một nhật ký trong Event Viewer, từ thực đơn View, lựa chọn Filter để hiển thị thẻ Filter trong hộp thoại Properties của

nhật ký sự kiện. Trong hộp thoại này, có thể chỉ định kiểu sự kiện nào muốn hiển thị và lựa chọn các sự kiện tiêu biểu để giảm bớt danh sách sự kiện về kích thước có thể quản lý được**.**

3.3 Truy cập nhật ký sự kiện từ xa

Sử dụng Event Viewer để xem các nhật ký trên các máy tính Window khác như là xem trên máy tính đang làm việc. Để thực hiện điều này, trong khung phạm vi, lựa chọn đối tượng Event Viewer (Local) và lựa chọn "Connect To Another Computer" (Kết nối tới máy tính khác) từ thực đơn Action. Trong hộp thoại Select Computer, chỉ ra tên của máy tính muốn xem các nhật ký sự kiện trên máy đó.

3.4.Lưu giữ các Nhật ký sự kiện

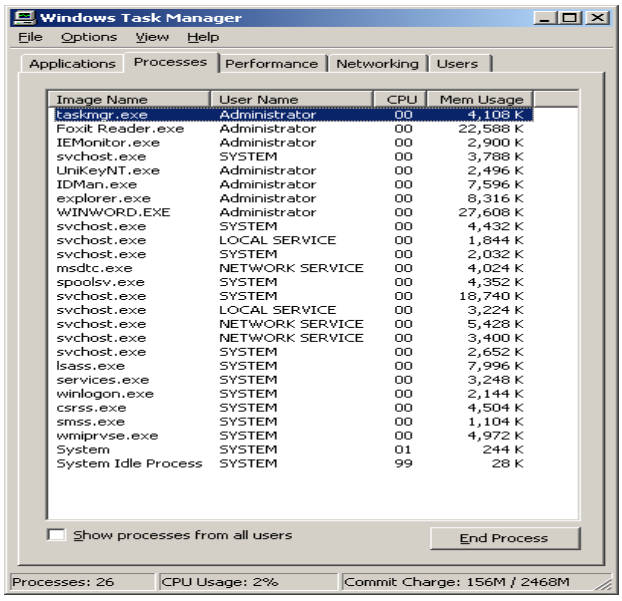
Snap-in Event Viewer có thể lưu các nhật ký thành file trong một số định dạng, bao gồm dạng văn bản (.txt), dạng bảng (.csv) và một định dạng nhật ký sự kiện có phần mở rộng là .evt, định dạng này có thể mở bằng snap-in.

4.Sử dụng Task Manager

4.1 Task Manager :(Trình Quản lý Tác vụ)

Hộp thoại Windows Task Manager theo mặc định sẽ chứa 5 thẻ:

- Applications (Ứng dụng)
- Processes (Tiến trình)
- Performance (Hiệu năng)
- Networking (Mạng)
- Users (người dùng)

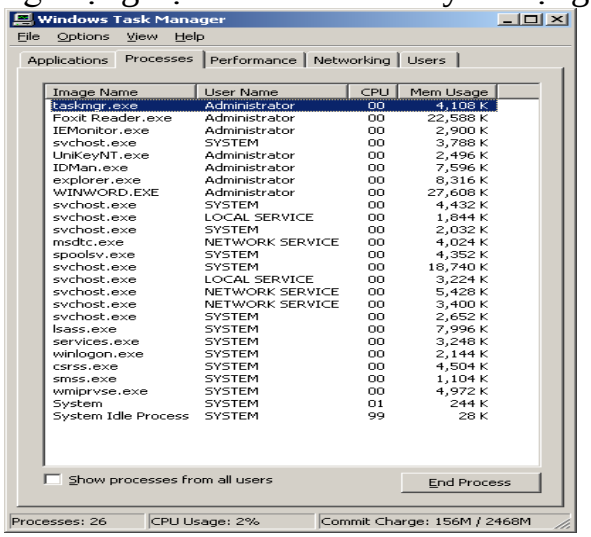

Windows Task Manager
File Options View Help
Applications Processes Performance Networking Users
Image Name User Name CPU Mem Usage
taskmgr.exe Administrator 00 4,108 K
Foxit Reader.exe Administrator 00 22,588 K
IEMonitor.exe Administrator 00 2,900 K
svchost.exe SYSTEM 00 3,788 K
UniKeyNT.exe Administrator 00 2,496 K
IDMan.exe Administrator 00 7,596 K
explorer.exe Administrator 00 8,316 K
WINWORD.EXE Administrator 00 27,608 K
svchost.exe SYSTEM 00 4,432 K
svchost.exe LOCAL SERVICE 00 1,844 K
svchost.exe SYSTEM 00 2,032 K
msdtc.exe NETWORK SERVICE 00 4,024 K
spoolsv.exe SYSTEM 00 4,352 K
svchost.exe SYSTEM 00 18,740 K
svchost.exe LOCAL SERVICE 00 3,224 K
svchost.exe NETWORK SERVICE 00 5,428 K
svchost.exe NETWORK SERVICE 00 3,400 K
svchost.exe SYSTEM 00 2,652 K
lsass.exe SYSTEM 00 7,996 K
services.exe SYSTEM 00 3,248 K
winlogon.exe SYSTEM 00 2,144 K
csrss.exe SYSTEM 00 4,504 K
smss.exe SYSTEM 00 1,104 K
wmiprvse.exe SYSTEM 00 4,972 K
System SYSTEM 01 244 K
System Idle Process SYSTEM 99 28 K
Show processes from all users
End Process
Processes: 26 CPU Usage: 2% Commit Charge: 156M / 2468M

Hình 2-2:màn hình Windows Task Manager

4.2 Giám sát các tiến trình

Thẻ Processes liệt kê tất cả các tiến trình của các người dùng hiện tại đang chạy trên máy tính. Khi bạn lựa chọn “Show Processes From All Users” (Hiển thị các tiến trình từ tất cả người dùng), bên cạnh các ứng dụng mức người dùng, danh sách này còn hiển thị cả các dịch vụ và các tiến trình hệ thống. Theo mặc định, danh sách này bao gồm các thông tin sau đây về mỗi tiến trình:

+ Image Name: Tên của file chạy tiến trình này.
+ User Name: Tên tài khoản người dùng là chủ nhân của tiến trình này
+ CPU: Phần trăm của bộ vi xử lý do tiến trình này sử dụng
+ Mem Usage: Dung lượng bộ nhớ tiến trình này sử dụng


Windows Task Manager
File Options View Help
Applications Processes Performance Networking Users
Image Name User Name CPU Mem Usage
taskmgr.exe Administrator 00 4,108 K
Foxit Reader.exe Administrator 00 22,588 K
IEMonitor.exe Administrator 00 2,900 K
svchost.exe SYSTEM 00 3,788 K
UniKeyNT.exe Administrator 00 2,496 K
IDMan.exe Administrator 00 7,596 K
explorer.exe Administrator 00 8,316 K
WINWORD.EXE Administrator 00 27,608 K
svchost.exe SYSTEM 00 4,432 K
svchost.exe LOCAL SERVICE 00 1,844 K
svchost.exe SYSTEM 00 2,032 K
msdtc.exe NETWORK SERVICE 00 4,024 K
spoolsv.exe SYSTEM 00 4,352 K
svchost.exe SYSTEM 00 18,740 K
svchost.exe LOCAL SERVICE 00 3,224 K
svchost.exe NETWORK SERVICE 00 5,428 K
svchost.exe NETWORK SERVICE 00 3,400 K
svchost.exe SYSTEM 00 2,652 K
lsass.exe SYSTEM 00 7,996 K
services.exe SYSTEM 00 3,248 K
winlogon.exe SYSTEM 00 2,144 K
csrss.exe SYSTEM 00 4,504 K
smss.exe SYSTEM 00 1,104 K
wmiprvse.exe SYSTEM 00 4,972 K
System SYSTEM 01 244 K
System Idle Process SYSTEM 99 28 K
Show processes from all users
End Process
Processes: 26 CPU Usage: 2% Commit Charge: 156M / 2468M

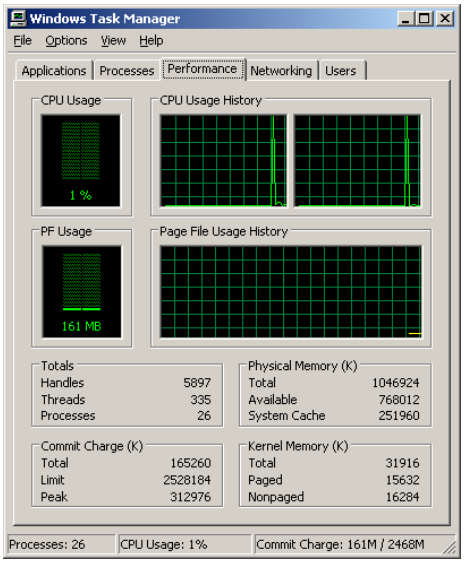
Hình 2-3:màn hình giàm sát tiến trình

Để giám sát thông tin dễ dàng về các tiến trình hệ thống, có thể thao tác chúng bằng Task Manager. Bằng cách nhấn phải chuột vào bất kì tiến trình nào trong danh sách, có thể thực hiện các tác vụ sau:

+ Set Priority (Thiết lập mức ưu tiên): Chỉnh sửa thời gian bộ vi xử lý sử dụng cho tiến trình đó trong mối tương quan với các tiến trình khác trong hệ thống
+ Set Proccessor Afinity (Thiết lập mối quan hệ vi xử lý): Chỉ định bạn muốn chạy tiến trình bằng bộ vi xử lý nào trên một hệ thống máy tính có nhiều bộ vi xử lý.
+ End Proccess (Kết thúc tiến trình): Dừng tiến trình ngay lập tức. Mọi tài nguyên chưa lưu sẽ bị mất
+ End Proccess Tree (Kết thúc cây tiến trình): Dừng mọi tiến trình và các tiến trình con hoặc tiến trình liên quan ngay lập tức. Mọi dữ liệu chưa lưu sẽ bị mất.
+ Debug (Gỡ lỗi): Tạo ra một trường hợp ngoại lệ để ngắt tiến trình và gắn nó với một trình gỡ lỗi được cài đặt trong hệ thống.

4.3 Giám sát mức hiệu năng

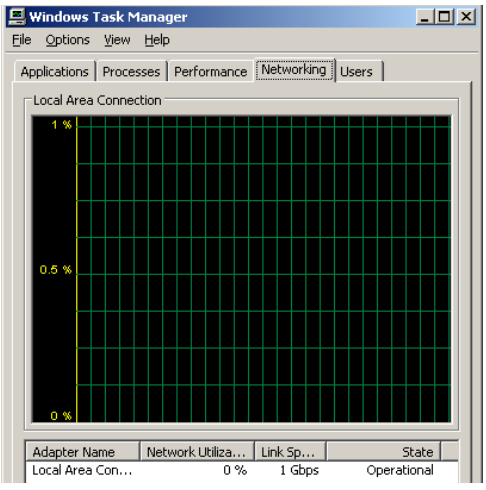
Nhấn đúp chuột vào một trong các đồ thị sẽ mở rộng nó theo chiều dọc (trục tung) để hiển thị các giá trị một cách rõ ràng hơn. Các hiển thị số bên dưới sẽ cho biết mức độ sử dụng bộ nhớ vật lý (Physical), bộ nhớ lõi (Kernel) và bộ nhớ cam kết (Commit), đồng thời cả số lượng các Handle (Liên kết giữa các tiến trình), Thread (Luồng), và các tiến trình đang hoạt động



Hình 2-4: Giám sát mức hiệu năng

4.4 Giám sát các hoạt động của mạng

Thẻ Networking cho thấy các kết nối mạng đang hoạt động theo tên, cùng với tốc độ kết nối, phần trăm băng thông sử dụng và trạng thái hoạt động của nó. Đồng thời có một đồ thị hiển thị băng thông sử dụng trong kết nối mạng đang chọn hiện tại.

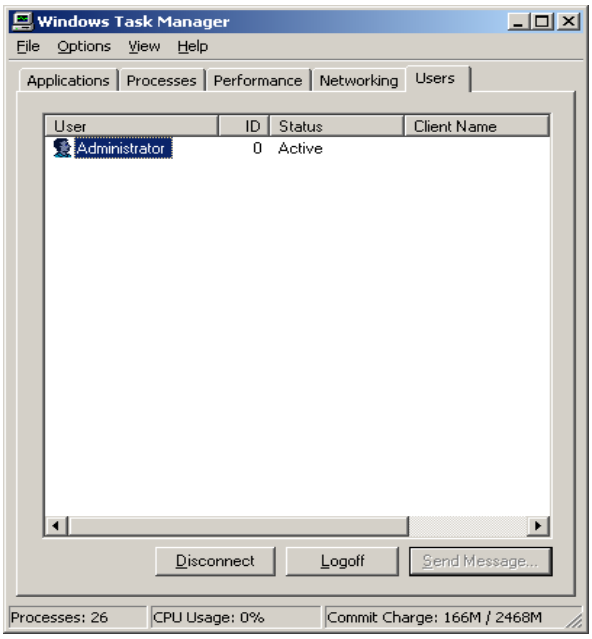


Hình 2-5:màn hình Giám sát các hoạt động của mạng

4.5 Giám sát người dùng

Thẻ Users sẽ liệt kê tất cả các người dùng đang đăng nhập vào máy tính. Các người dùng đăng nhập có thể là người dùng làm việc trực tiếp tại màn hình

điều khiển hoặc người dùng đăng nhập qua kết nối từ xa trên mạng. Sử dụng các điều khiển trong thẻ này có thể đăng xuất người dùng đó, ngắt kết nối của họ đến máy tính hoặc gửi thông báo cho họ.


Windows Task Manager
File Options View Help
Applications Processes Performance Networking Users
User ID Status Client Name
Administrator 0 Active
Disconnect Logoff Send Message...
Processes: 26 CPU Usage: 0% Commit Charge: 166M / 2468M

Hình 2-6:màn hình Giám sát người dùng

Bài tập thực hành

Bài tập 1: AUDIT POLICY - Windows server 2012

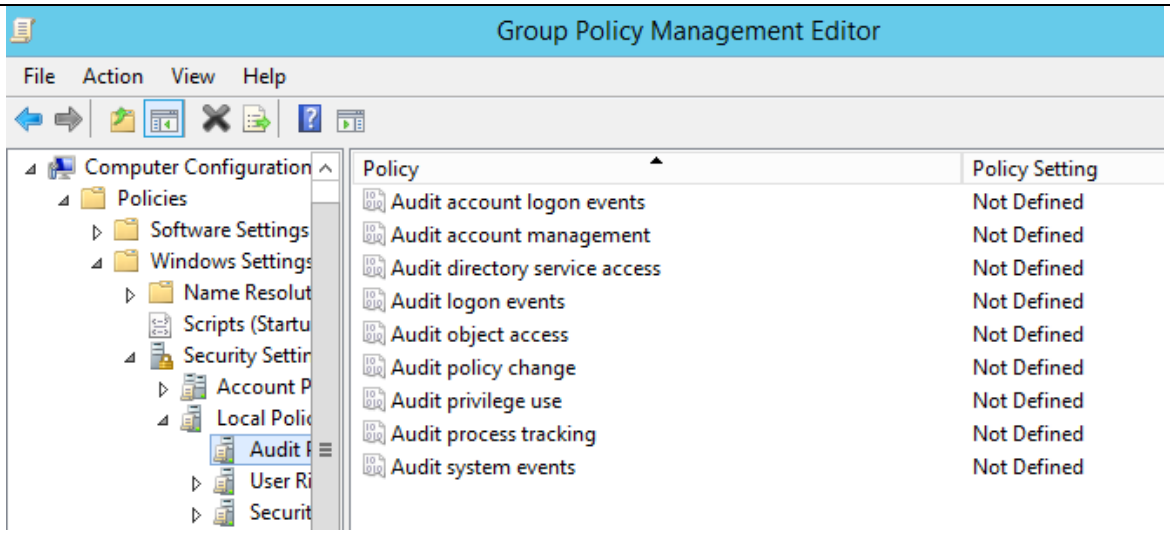
Yêu cầu: Triển khai Audit Policies và giám sát việc đó bằng Event Viewer trên nền Windows Server 2012

Chuẩn bị:

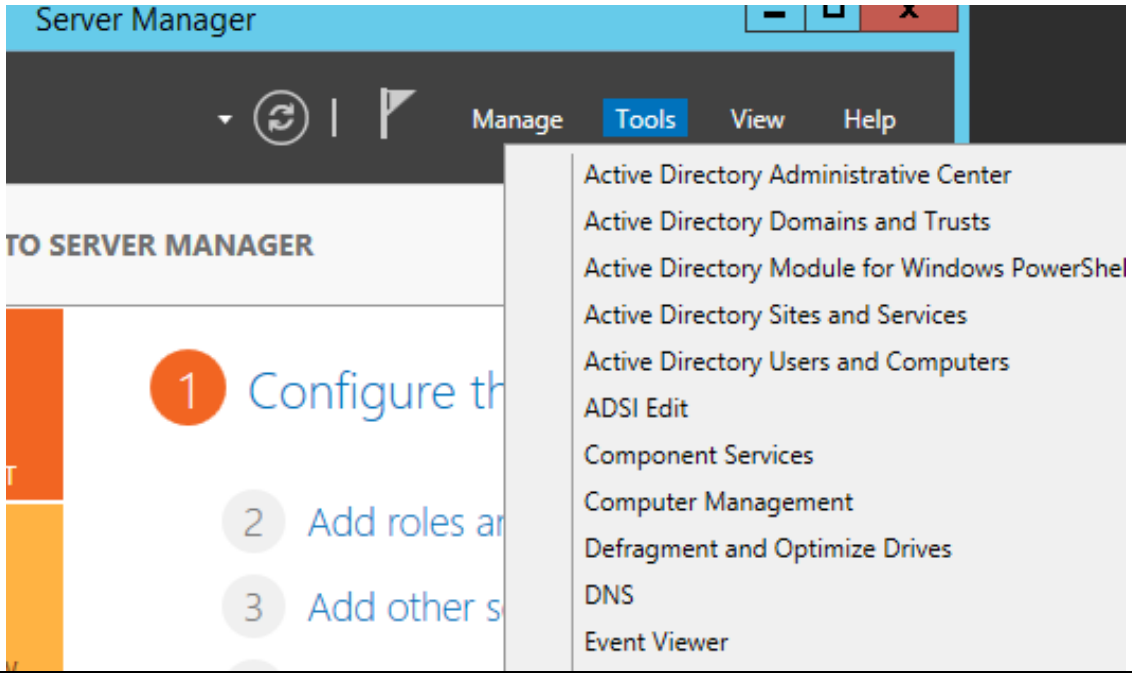
- 1 máy đóng vai trò Domain Controller + File server: **2012may1**
- 1 máy computer domain : **2012may2**
- Vào ổ C → tạo folder: Logs.

Thực hiện

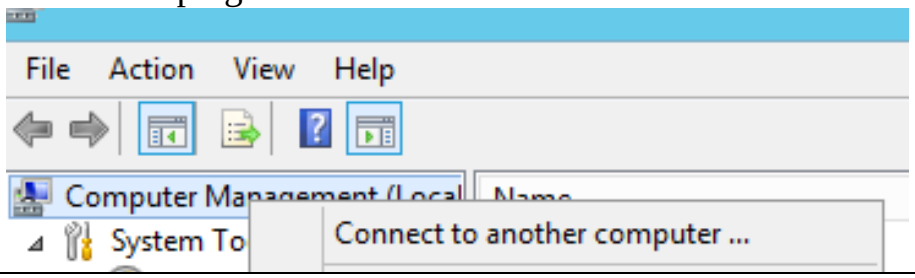
Bước 1: Default Domain Controllers Policy → Edit → Computer Configuration (audit policy chỉ có ở mục này) → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy.



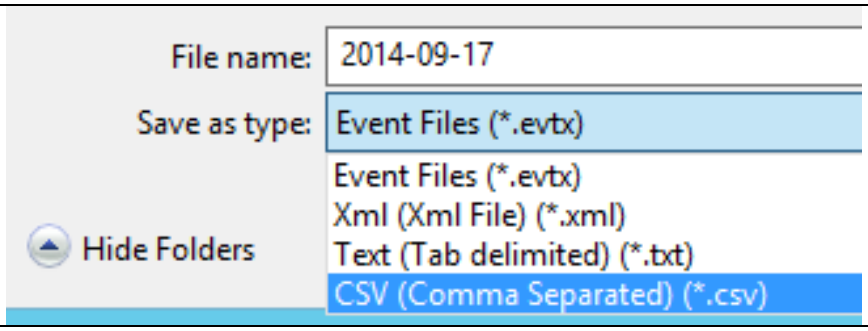
Bước 2: Server Manager → Tools → Event Viewer.



Bước 3: Run → compmgmt.msc → Event Viewer

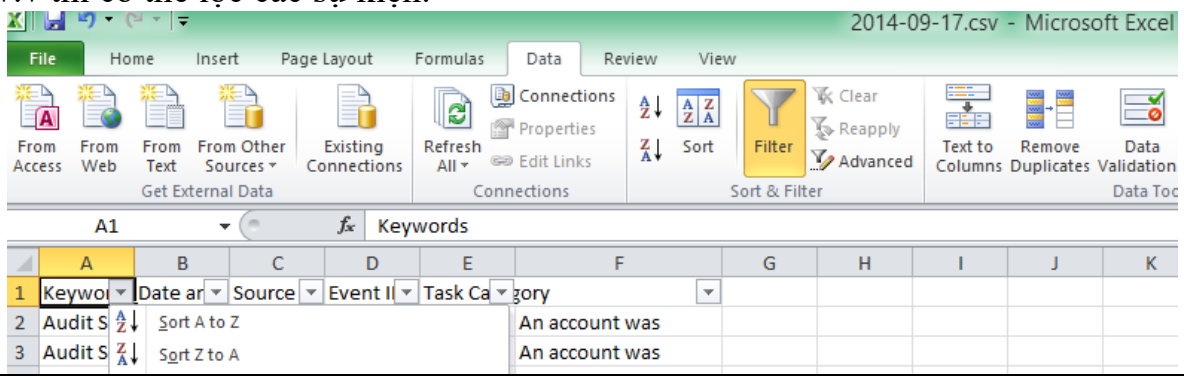


Bước 4: Security → chuột phải Save All Events As …



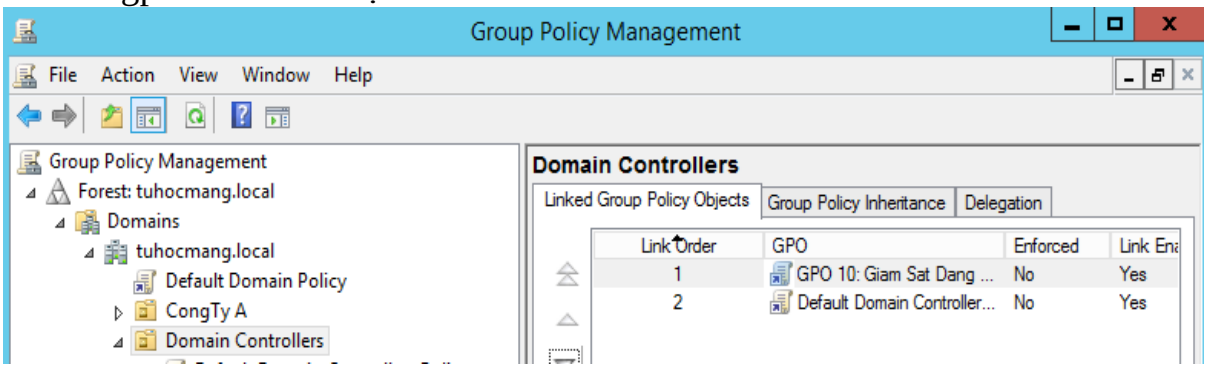
Bước 5: Hệ thống cho phép ta lưu log dưới dạng file

Event Files (*.evtx): chỉ có thể đọc log file này bằng Event Viewer→ **CSV (*.csv)**: cũng có thể đọc bằng các chương trình soạn thảo, nhưng các sự kiện trong file được cách nhau bằng phím tab. Nếu dùng phần mềm Exell hay Acess v.v thì có thể lọc các sự kiện.

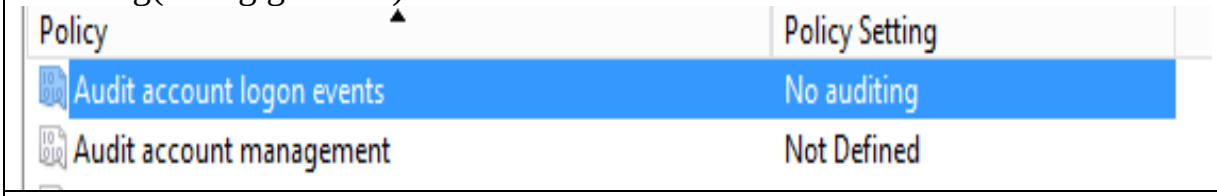


Bước 6: Tình huống 1: Giám sát người dùng đăng nhập không thành công trên hệ thống → tạo GPO tác động lên OU chứa DC.

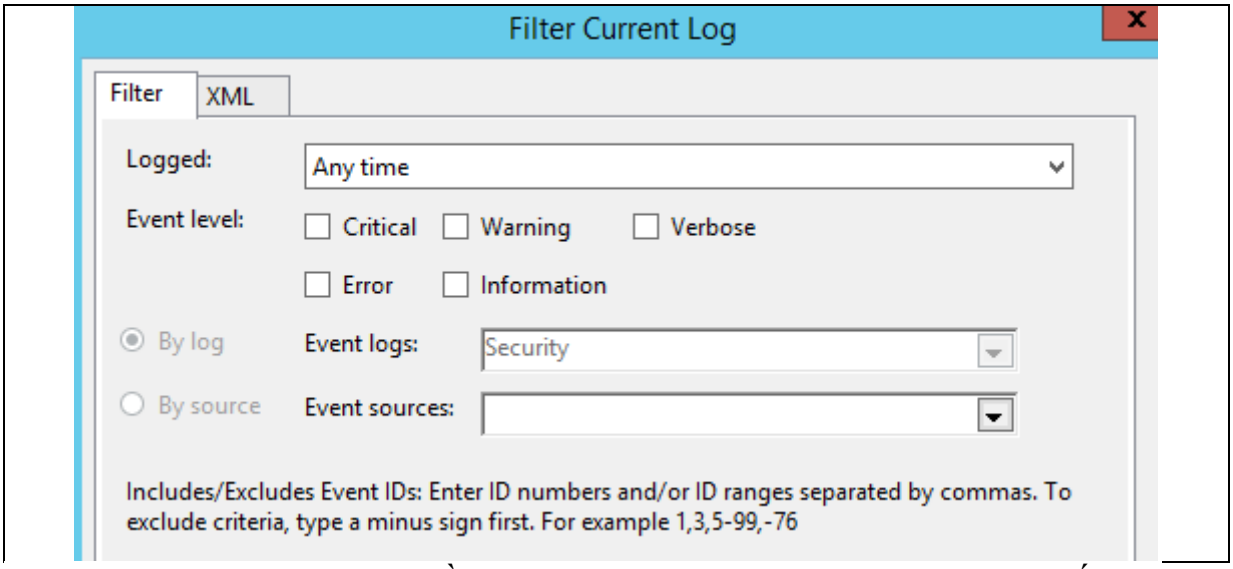
Run → gpmc.msc → chọn OU Domain Controller → Create a GPO …



Bước 7: Logon Events → Double click → Check vào Define these policy settings , ta bỏ check success và failure thì policy xuất hiện trạng thái No Auditing(không giám sát)



Bước 8: Windwos Logs →phải chuột Security → Filter Current Log ….



Bài tập 2: Xác định thành phần nào gây ra hiện tượng hoạt động kém đối với server. CPU, Ram, Ổ cứng.

Yêu cầu: Giám sát hoạt động của server về phần cứng

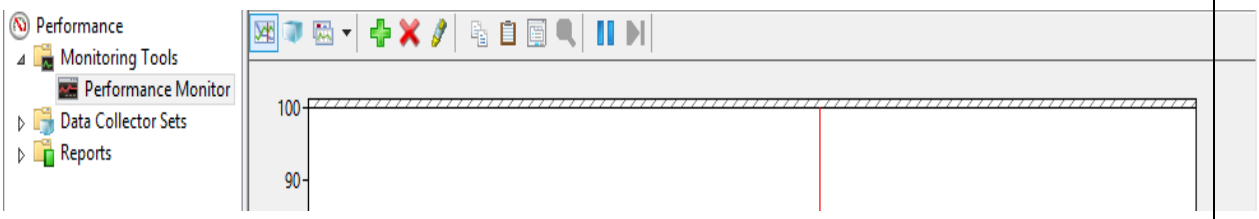
Chuẩn bị:

- 1 máy đóng vai trò Domain Controller 2012may1
- 1 máy computer domain : 2012may2

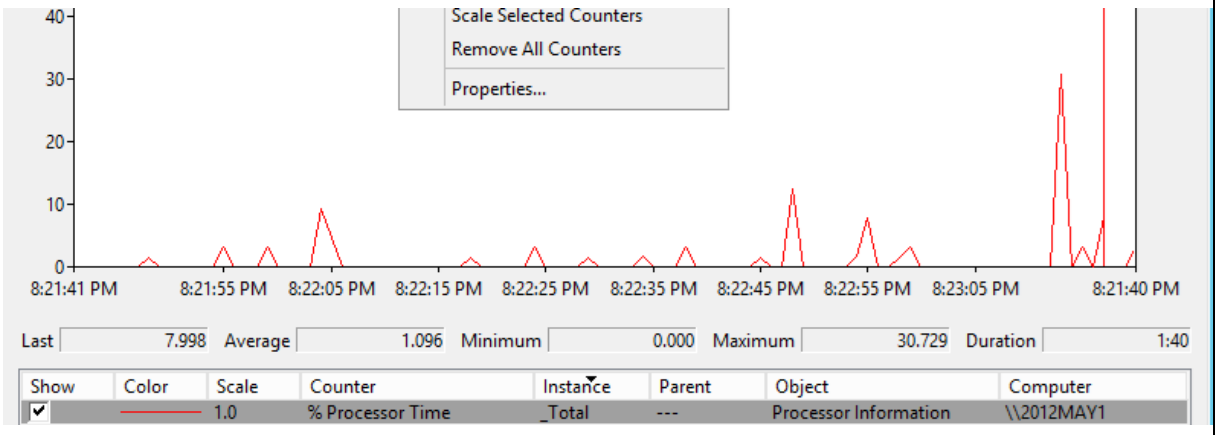
Thực hiện

1.Real Time Mode (giám sát theo thời gian thực)

Bước 1:Dùng Performance Monitor

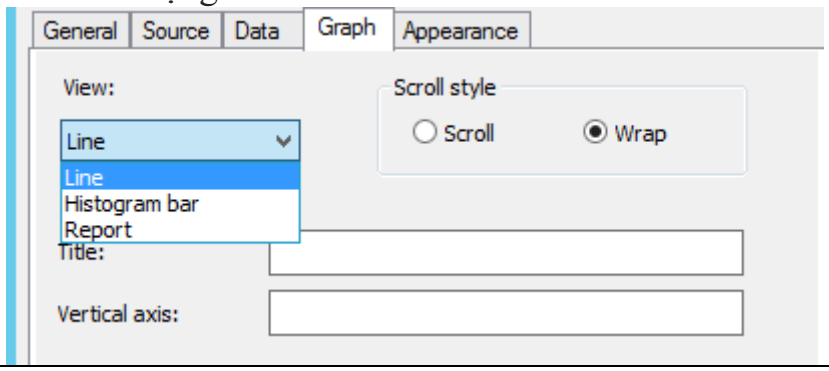


Bước 2: Chọn vào đồ thị → Properties

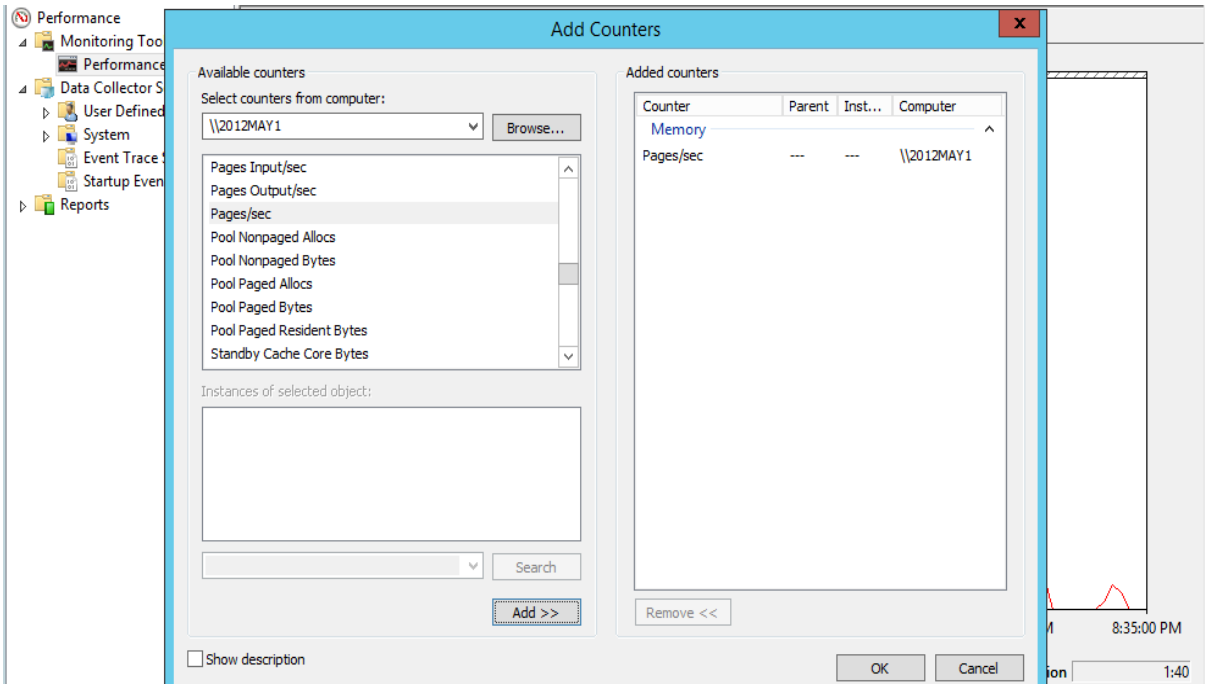


Bước 3: Tab Grap, bung View, Windows cung cấp co ta 3 dạng biểu đồ để

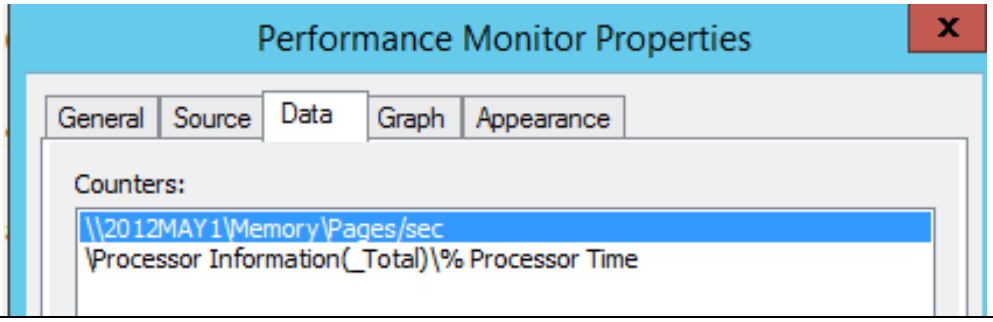
giám sát
+ Line: dạng đồ thị (mặc định)
+ Histogram Bar: dạng biểu đồ cột
+ Report : chỉ xuất ra dạng số



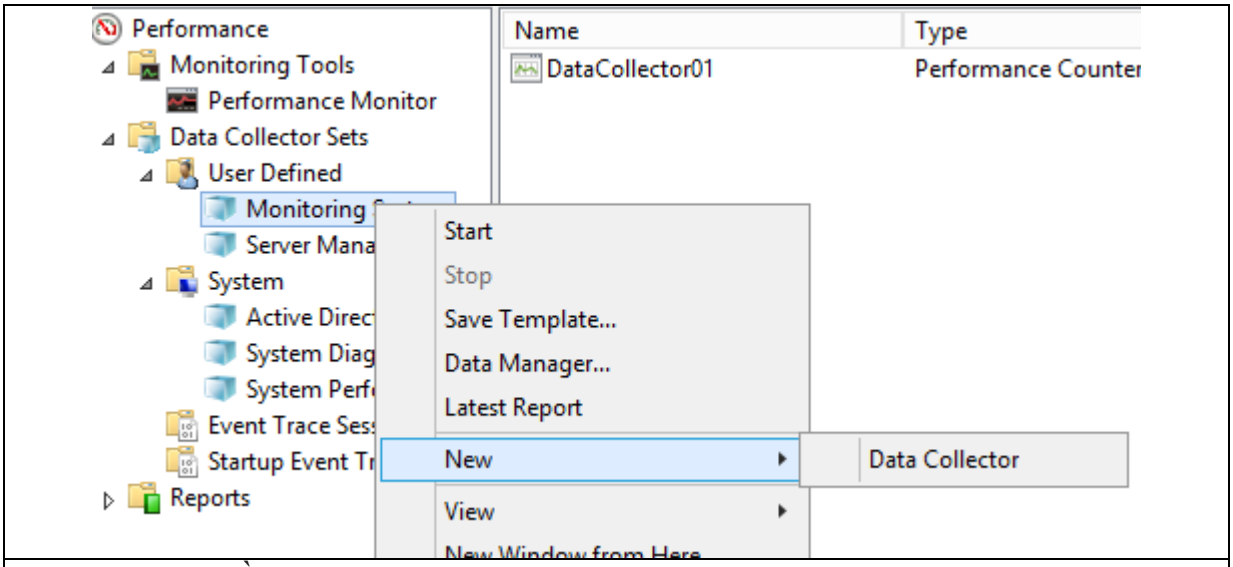
Bước 4: Mặc định Performance Monitor chỉ giám sát CPU theo thời gian thực, muốn xem các chỉ số khac ta làm như sau. Chọn vào đồ thị →Add counters. Giả sử ta muốn giám sát them Memory (add Pages/sec)



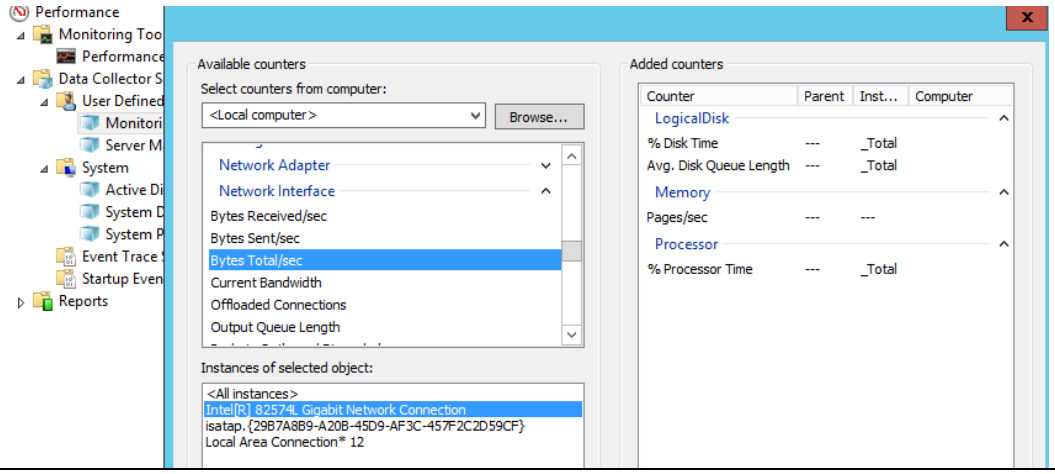
Bước 5: Các thành phần giám sát sẽ chung 1 bảng đồ thị (chung 1 hệ trục), ta cần đổi màu cho từng thành phần→Pages/sec → Properties → Tab Data



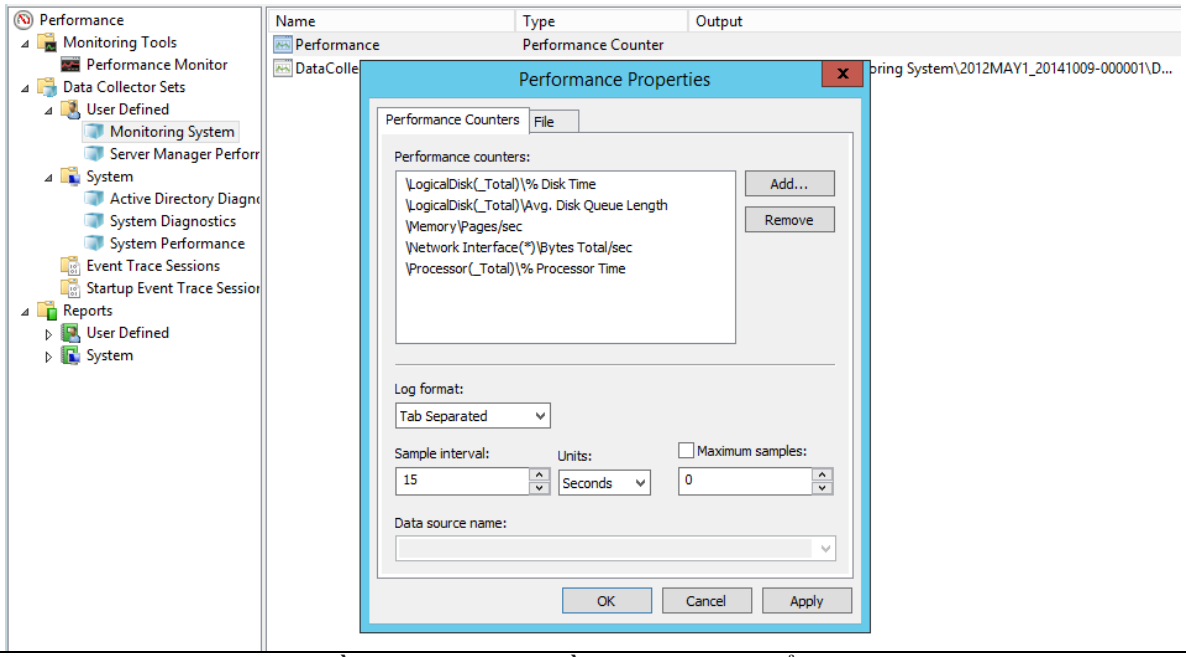
Bước 6: Chọn vào Monitoring System vừa tạo → New → Data Collector



Bước 7: Cửa sổ Create New Data Collector → Add



Bước 8: Chọn vào Data Collector " Performance" vừa tạo → properties Log Format: chọn Tab Seperated để có thể đọc file log bằng phần mềm Microsoft Excel.



Bước 9: Sau đó stop rồi mở log file bằng excel→ Để cột Network có giá trị thì

chúng ta phải copy 1 file nào đó qua mạng (từ server qua client).

	(PDH-TSV 4.0)	\\2012MAY1\LogicalDisk(_Tota	\\2012MAY1\LogicalDisk(_Total)\Avg. Disk Que	\\2012MAY1\Memory\Pages/se	\\2012MAY1\Network Inter	\\2012MAY1\Netw	\\2012MAY1\I	\\2012MAY1\Proce
2	32:45.8							
3	33:00.8	0.429474985	0.0085895	0	0	0	1.766356865	
4	33:15.8	0.098436373	0.001968727	0	64.06717292	0	0.103765285	
5	33:30.8	0.162165298	0.003243306	0	0	0	0.10351274	
6	33:45.8	0.024691972	0.000493839	0	44.57901344	0	0.001683726	
7	34:00.8	0.589659555	0.011793191	0	22.26638339	0	0.313702217	
8								

5.TÓM TẮT NỘI DUNG

- Sử dụng nhật ký các biến đếm để thiết lập một đường cơ sở cho hiệu năng hệ thống và sau đó đều đặn kiểm tra các nhật ký này xem sai lệch so với đường cơ sở chuẩn
- Giám sát trạng thái hoạt động của các dịch vụ mạng
- Giám sát các tài nguyên các máy phục vụ và các thiết bị đầu cuối
- Giám sát các thông số an toàn thiết bị phần cứng trên host như: nhiệt độ CPU,tốc độ quạt, pin, giờ hệ thống
- Cảnh báo cho người quản trị bằng nhiều hình thức như email, tin nhắn tức thời(IM), âm thanh …nếu như có thiết bị, dịch vụ gặp trục trặc
- Tổng hợp, lưu giữ và báo cáo định kỳ về tình trạng hoạt động của mạng.

6. CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày các giám sát hiệu năng, giám sát mạng và giám sát người dùng.

Câu 2: Trình bày tinh chỉnh và giám sát mạng Windows server

1. Sử dụng event viewer
2. Sử dụng task manager
3. Sử dụng performance console

Câu 3: Hệ thống giám sát mạng là gì? Chức năng và vai trò của nó trong quản trị mạng?

BÀI TẬP

Bài tập 1: Windows Performance Monitor 2012 cung cấp một giao diện tuỳ biến mang đến khả năng phân tích, tìm kiếm, phân loại dữ liệu và hoạt động của hệ thống sau đó báo cáo tình trạng cho người quản trị.

Yêu cầu: Tạo một Performance Monitor để quản trị hệ thống trên Windows Server 2012 R2.

Chuẩn bị: 1 máy PC cài đặt win server 2012 R2

Hướng dẫn làm bài:

B1: Chọn Server Manager trên thanh taskbar hoạt nhấn tổ hợp phím "ctrl + Q" và gõ tên "Server Manager".

B2: Tại Server Manager, phía trên bên phải ta chọn công cụ Tools và click chọn Performance Monitor

B3: Data Collector Set, User Define →User Define → New Data Collector Set để tạo một tập hợp những phần tử của hệ thống mà chúng ta muốn quản lí

B4: Create manually→Next→ What type of data do you want to include? → Performance counter→ Next→Add

B5: Bandwitch và Processor Time để xem quá trình hoạt động của hardware như Network và processor và lần lượt nhấp chọn "add"→OK

B6: Sample interval → mặc định là 15 giây→ Next → Finish.

B7: Nhấp phải Server Performance→start→ stop → Reports", "User Defined", "Server Performance" → log mới nhất để xem quá trình hoạt động đã được ghi lại.

Bài tập 2: PAM (IP Address Management) là tính năng đã được giới thiệu từ Windows Server 2012 cung cấp khả năng quản lý và giám sát tùy biến cao cho các cơ sở hạ tầng địa chỉ IP trong hệ thống mạng.

Yêu cầu: Cài đặt, cấu hình IPAM để phát hiện, theo dõi, giám sát và quản lý không gian địa chỉ IP được sử dụng trên mạng.

Chuẩn bị:

- DC2012: Domain Controller (domain mcthub.local) chạy Windows Server 2012 đã được cài đặt và cấu hình DHCP
- SERVER1: Domain Member chạy Windows Server 2012

Hướng dẫn làm bài:

1. Cài đặt IPAM

B1: Trên máy DC2012→Active Directory Users and Computer→ SERVER1 (IPAM Server) vào danh sách thành viên group Event Log Reader

B2: SERVER1→ cài đặt feature IP Address Management→Server Manager →Add Role and Features

B3: Select Features: Chọn IP Address Management (IPAM) Server→ Cài đặt các Feature cần thiết→ Install

2. Cấu hình IPAM

B1: rên máy SERVER1→Kết nối đến IPAM Server → Connect to IPAM Server→ SERVER1.mcthub.local → OK

B2: Rovision the IPAM Server →IPAM→Next→ Group Policy Based → GPO name prefix →Next→ Apply→ Close

B3: Configure server discovery→domain→Add→OK

B4: Start server discovery→ Select or add to manage and verify IPAM Access → DHCP và DNS Server cần quản lý

B5: DC2012 – Edit Server→ Manageability thành Managed → OK→ Blocked

B6: DC2012 và SERVER1, cập nhật Policy bằng lệnh GPUPDATE /FORCE

B7: GPRESULT /R để kiểm tra kết quả áp đặt GPO, bảo đảm rằng máy DC2012 được áp dụng 3 GPO là IPAM_DNS, IP_DHCP và IPAM_DC_NPS.

B8: Refresh Server Access Status→ Unblocked → Retrieve All Server Data

BÀI 3: KHÔI PHỤC SERVER KHI BỊ HỎNG

Mã bài:MĐ 24-03

Thời gian: 5 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Đưa ra được các biện pháp phòng ngừa
- Có khả năng sử dụng các biện pháp sao lưu dự phòng có hiệu quả
- Có khả năng tìm Pan phần cứng
- Giải quyết được các trục trặc trong quá trình khởi động
- Sửa chữa được bản phần mềm cài đặt hỏng.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1.Các biện pháp phòng ngừa

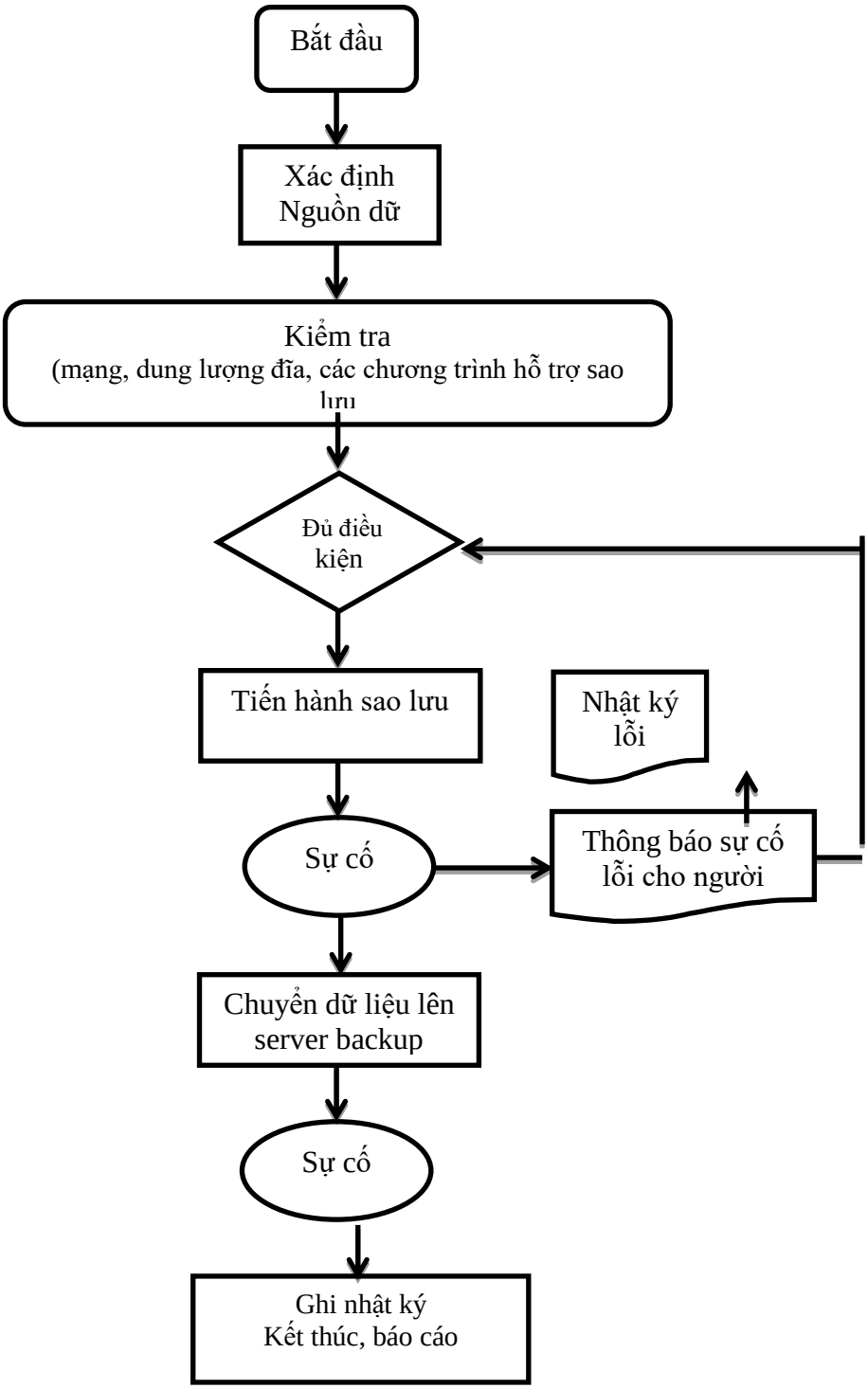
Cách lựu chọn sao lưu dự phòng:

Chức năng cơ bản nhất của một chương trình phần mềm sao lưu là cho phép lựa chọn cái gì muốn sao lưu, đôi khi còn được gọi là mục tiêu (Target). Một chương trình sao lưu tốt cho phép làm việc này theo rất nhiều cách. Trong hầu hết các trường hợp, có thể lựa chọn:

+ Toàn bộ máy tính
+ Các đĩa cứng xác định trong một máy tính
+ Các thư mục xác định trong một đĩa cứng
+ Các file xác định trong một thư mục

2.Các phương pháp sao lưu dự phòng

2.1 Lưu đồ



Hình 3-1: sơ dồ backup

2.2 Diễn giải lưu đồ

Bước 1: Xác định nguồn dữ liệu sao lưu:

Khi cần thiết phải sao lưu phần dữ liệu nào của hệ thống trước thời gian sao lưu tự động theo lập lịch để phục vụ cho các tác vụ cấp bách trên hệ thống, người được phân công liệt kê các loại dữ liệu được sao lưu vào file

backup_filetype.txt. Chương trình sao lưu sẽ đọc các thông số trong tập tin này để tiến hành sao lưu.

Bước 2: Kiểm tra (mạng, ftp, dung lượng đĩa cứng, tập tin và thư mục đã backup):

Việc kiểm tra nhằm tăng thêm độ an toàn cho dữ liệu được sao lưu, các bước kiểm tra sẽ được đóng gói thành tập tin script.sh.

Bước 3: Tiến hành sao lưu:

Sau khi đã thực hiện các bước chuẩn bị và kiểm tra, nếu đủ điều kiện thì hệ thống sẽ thực hiện các tác vụ để sao chép dữ liệu trên server. Nếu việc sao lưu không thành công thì báo cáo với admin (qua email kèm thông báo lỗi) đồng thời tìm hướng khắc phục lỗi.

Bước 4: Chuyển dữ liệu lên server backup:

Sau khi các tác vụ sao chép thành công, tiến hành việc truyền dữ liệu vào Backup server để lưu trữ. Nếu xảy ra lỗi trong quá trình truyền dữ liệu, hệ thống sẽ ghi logs vào tập tin ftp_log.txt đồng thời người được phân công cần thực hiện lại các khâu kiểm tra như bước 2, sau đó, thực hiện đồng bộ dữ liệu trên hai ỗ cứng lưu trữ.

Bước 5: Ghi nhật ký sao lưu(logs):

Sau khi quá trình sao lưu dữ liệu thành công, hệ thống sẽ tự động cập nhật các thông tin sao lưu thành công vào tập tin logs_bk.txt

Bước 6: Báo cáo người quản lý:

Người được phân công sẽ lập báo cáo tuần và tháng về tình hình sao lưu, đồng thời kèm theo tập tin logs_bk.txt để người quản lý nắm được tình hình sao lưu dễ dàng hơn.

3.Tìm và quản trị Pan phần cứng bằng công cụ System Information

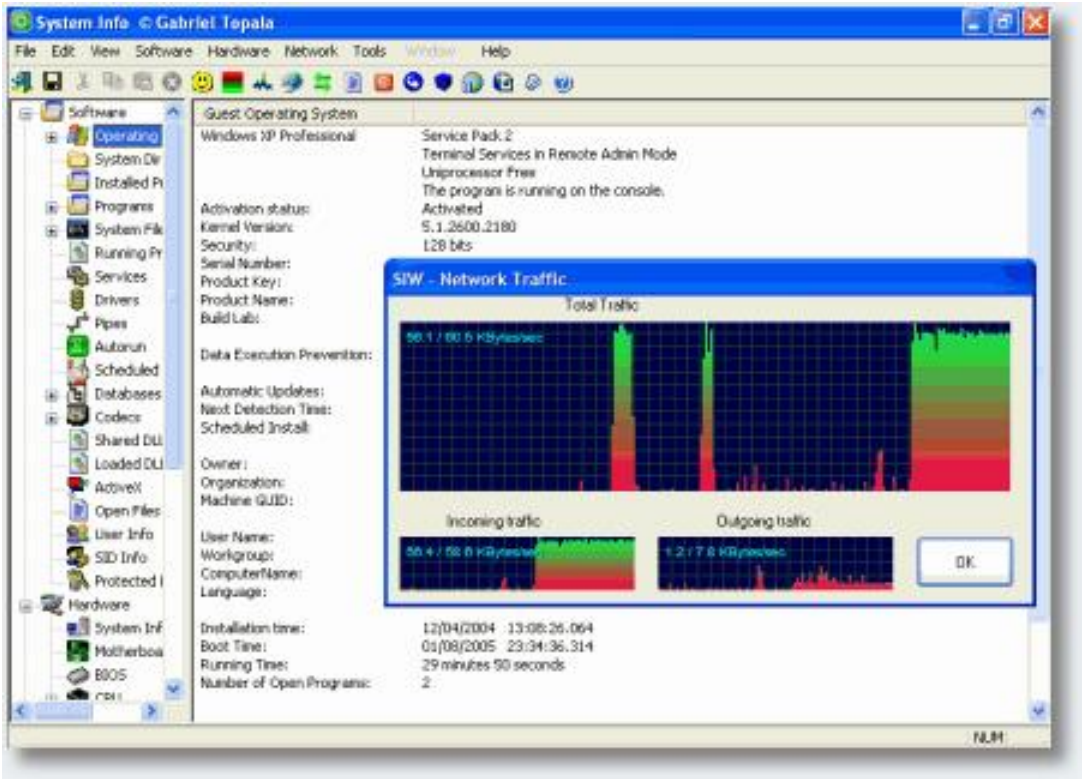
Phần mềm: gồm hệ điều hành, các phần mềm đã cài đặt, các bản vá, tiến trình, dịch vụ, người dùng, …

Phần cứng: gồm CPU, bo mạch chủ, RAM, BIOS, video card, …

Mạng: gồm card mạng, các tài nguyên được chia sẻ, những cổng đang mở, …

Công cụ khác: gồm khôi phục dữ liệu đã xóa, xem password dạng dấu sao (*), thay đổi địa chỉ MAC, …

Theo dõi ở chế độ Real-time CPU, bộ nhớ, network traffic, …



Hình 3-2: công cụ System Information

4.Giải quyết các trục trặc trong quá trình khởi động

Trước khi vào Windows thì có thể máy tính gặp vấn đề về phần cứng. Test các bộ phận của máy tính một cách riêng biệt nhằm phát hiện thiết bị nào bị lỗi để có thể thay thế. Nên bắt đầu từ nguồn, Ram, đến card màn hình, rồi đến chip, mainboard…

Các lỗi thường gặp:

+ 8024 Gate - A20 Error: Lỗi bàn phím (có thể do kẹt phím).
+ Bad Partition Table: Lỗi do đĩa cứng được tạo và phân vùng partition bằng lệnh fdisk không đúng
+ A: Drive Error: Lỗi do các thông số đĩa cứng không được khai báo đúng trong CMOS.
+ Cmos Memory Size Mismatch: Lỗi do hỏng các chip nhớ hoặc RAM cắm không chắc.
+ Disk Boot Error, Replace And Strike To Retry: Lỗi do máy tính không tìm thấy đĩa có thể khởi động (chứa file khởi động của hệ điều hành).
+ Disk Drive 0 Seek Failure: Lỗi do dây cáp Data của ổ đọc đĩa lỗi, hoặc do mạch điều khiển bị lỗi.
+ Disk Boot Failure: Lỗi do đĩa khởi động bị hỏng hãy thay đĩa khởi động khác.

+ Disk Read Failure - Strike F1 To Retry Boot: Lỗi do đĩa hỏng, cắm nhầm cáp.
+ Hard Disk Failure: Lỗi do một trong các nguyên nhân sau: mạch điều khiển đĩa cứng hỏng, dây nguồn không gắn vào ổ cứng, cáp data cắm sai đầu, hoặc Jumper chọn master/sleve không đúng.
+ Keyboard Stuck Key Failure hay Keyboard Error: Lỗi do cắm bàn phím hỏng, hoặc kẹt phím.
+ RAM Test Address Failure: Lỗi do chip dùng địa chỉ hóa bộ nhớ hỏng, vì các chip này được tích hợp trên mainboard, nên phải sửa hoặc thay mianboard.

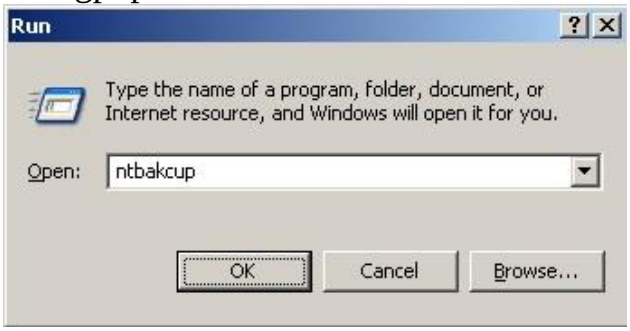
Bài tập1: Thực hành Backup AD và DHCP

Yêu cầu: Backup AD và DHCP

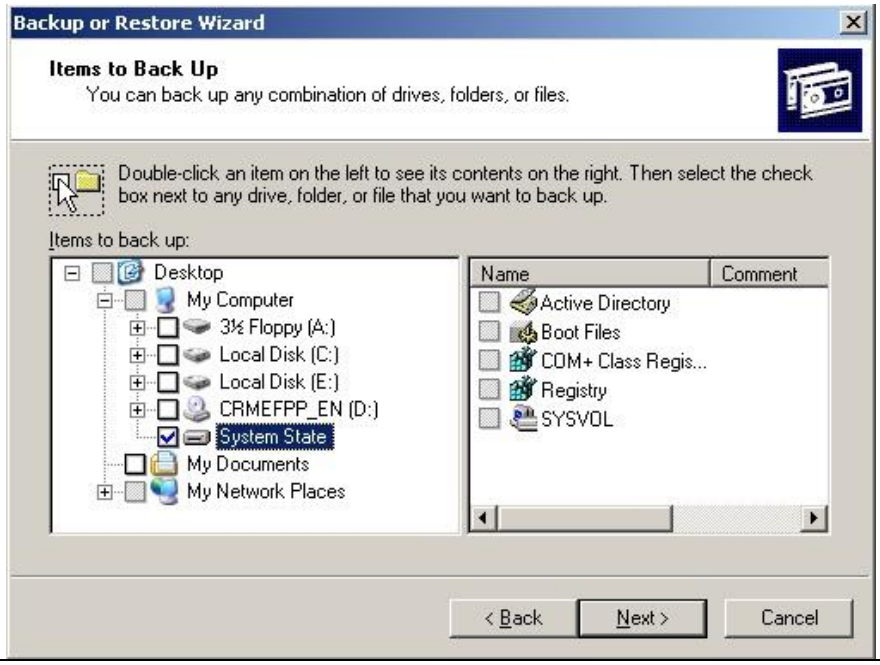
Chuẩn bị: 1 máy PC cài đặt w2k3 và nâng lên DC. Cài đặt, cấu hình DHCP

Thực hiện

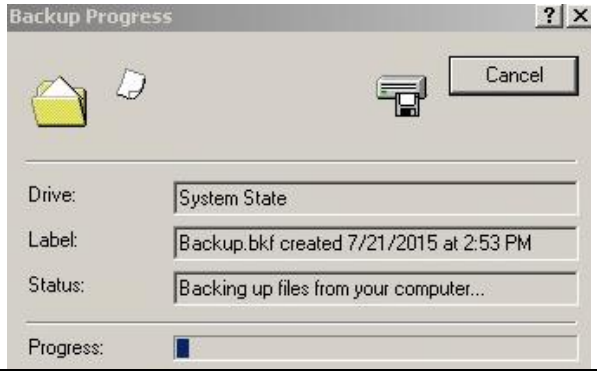
Bước 1: Tạo 2 user → gpupdate /force→ Run → cmd → ntbackup →OK



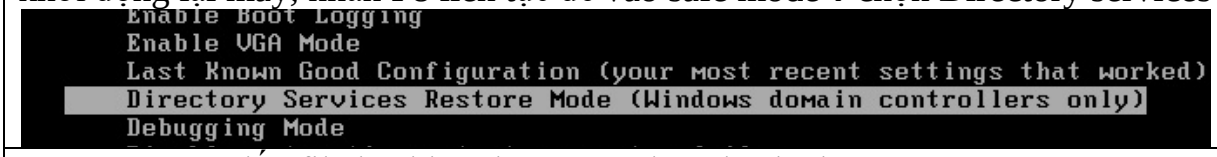
Bước 2: Chọn next→ backup→ Next→ let me → Next→ System State →Next→ browse tới nới cần lưu


Backup or Restore Wizard
Items to Back Up
You can back up any combination of drives, folders, or files.
Double-click an item on the left to see its contents on the right. Then select the check box next to any drive, folder, or file that you want to back up.
Items to back up:
Desktop
My Computer
3½ Floppy (A:)
Local Disk (C:)
Local Disk (E:)
CRMEFPP_EN (D:)
System State
My Documents
My Network Places
Name
Comment
Active Directory
Boot Files
COM+ Class Regis...
Registry
SYSVOL
< Back
Next >
Cancel

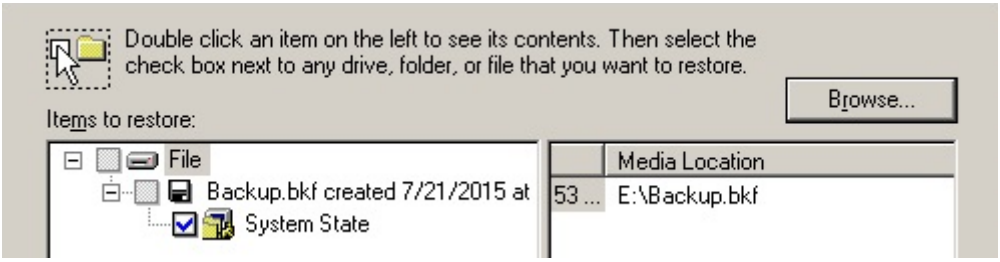
Bước 3: Chọn Advance→ Daily →backup hằng ngày →Next→ Verify data → Next→ Finsh→ Quá trình backup đang diễn ra



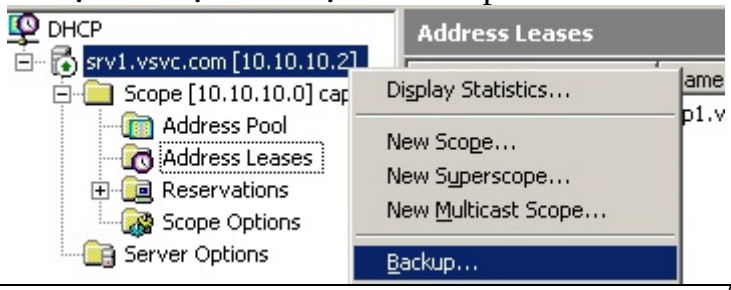
Bước 4: tiếp theo restore AD
khởi động lại máy, nhấn F8 liên tục đề vào safe mode→chọn Directory services


Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration (your most recent settings that worked)
Directory Services Restore Mode (Windows domain controllers only)
Debugging Mode

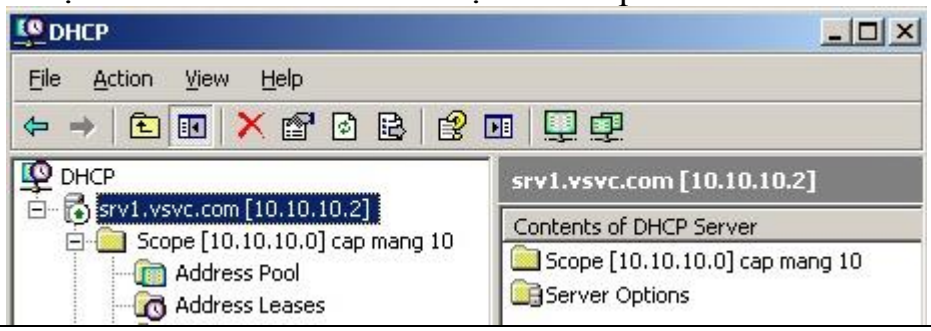
Bước 5: Tìm đến file backkup lưu trước đó. check chọn System state →Next→ finish


Double click an item on the left to see its contents. Then select the check box next to any drive, folder, or file that you want to restore.
Browse...
Items to restore:
File
Backup.bkf created 7/21/2015 at
System State
Media Location
53 ...
E:\Backup.bkf

Bước 6: Backup DHCP→click phải lên srv1,vsvc.com →Backup
tìm nơi cần lưu.Ví dụ: ổ E: tạo thư mục "bk dhcp" thì chỉ đến "bk dhcp"



Bước 7: Sau khi backup xong ta xóa scope đã tạo trước đó và tiến hành restore click phải chọn restore→ Chỉ đến thư mục "bkdhcp" trước đó →OK



Bài tập 2: Thực hànhTạo và quản lý máy ảo với Hyper-V trên Windows Server 2008

Yêu cầu: Tạo và quản lý máy ảo với Hyper-V trên Windows Server 2008

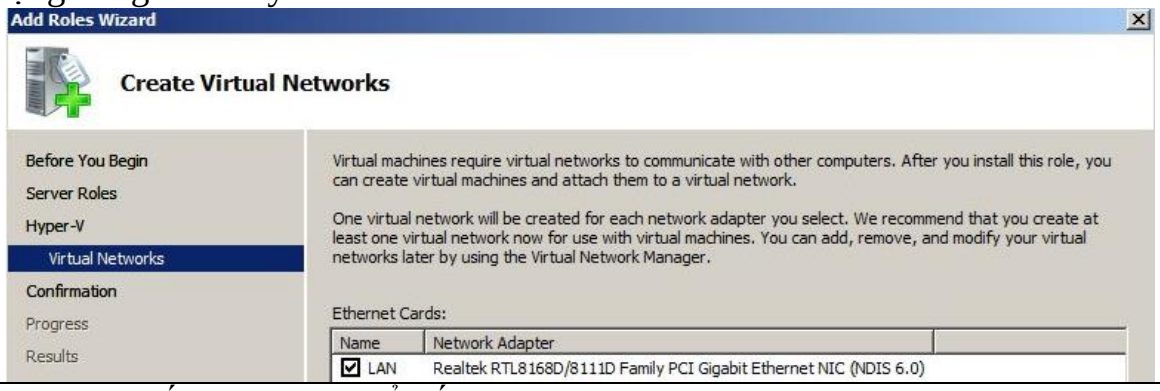
Chuẩn bị: 1máy PC cài win2k8, tải Hyper-V

Thực hiện

http://www.intel.com/support/process.../CS-014921.htm

Cài đặt HYPER-V

Bước 1: Mở Server Manager -- Roles → Add Role→ Hyper-V →Next→ Card mạng dùng cho máy ảo →Next

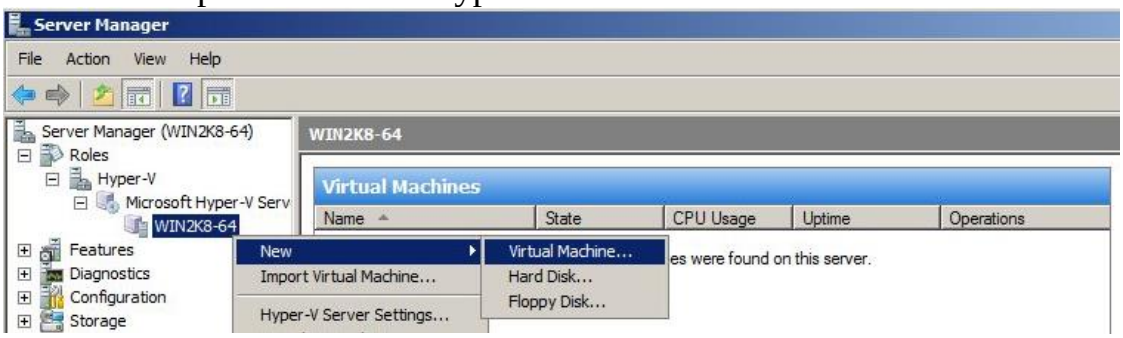

Add Roles Wizard
Create Virtual Networks
Before You Begin
Server Roles
Hyper-V
Virtual Networks
Confirmation
Progress
Results
Virtual machines require virtual networks to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual network.
One virtual network will be created for each network adapter you select. We recommend that you create at least one virtual network now for use with virtual machines. You can add, remove, and modify your virtual networks later by using the Virtual Network Manager.
Ethernet Cards:
Name
Network Adapter
LAN
Realtek RTL8168D/8111D Family PCI Gigabit Ethernet NIC (NDIS 6.0)

Bước 2: Nhấn nút Install để tiến hành cài đặt→ Restart máy → Close

Add Roles Wizard
Do you want to restart now?
This server must be restarted to finish the installation process. You cannot add or remove other roles, role services, or features until the server is restarted.
Yes
No

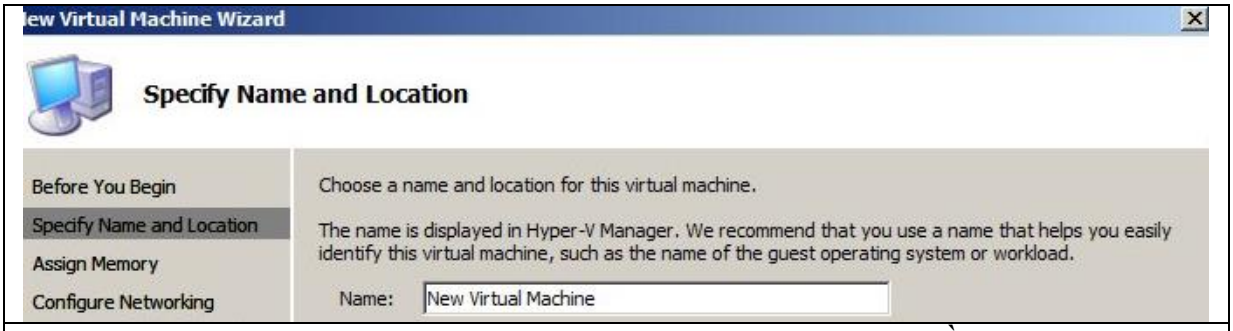
2. Tạo và cài đặt máy ảo

Bước 1: Click phải Microsoft Hyper-V Server →Connect to Server

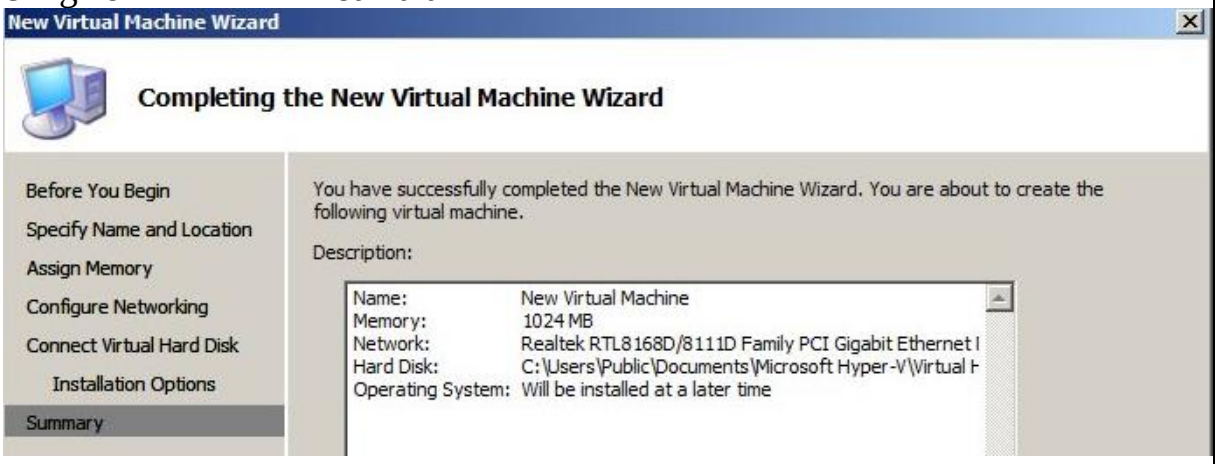


Chọn Local Computer →OK→ Click phải lên tên Server →New →Virtual Machine

Bước 2: Đặt tên cho máy ảo, có thể chỉ định thư mục lưu máy ảo bằng cách đánh dấu Store the virtual machine in a different location


New Virtual Machine Wizard
Specify Name and Location
Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Choose a name and location for this virtual machine.
The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.
Name:
New Virtual Machine

Bước 3: Qui định dung lượng RAM dành cho máy ảo (Tính bằng đơn vị MB)→ hiệu Card mạng dùng cho máy ảo→ tên File, vị trí lưu và dung lượng ổ cứng ảo→ Finish để hoàn tất


New Virtual Machine Wizard
Completing the New Virtual Machine Wizard
Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.
Description:
Name: New Virtual Machine
Memory: 1024 MB
Network: Realtek RTL8168D/8111D Family PCI Gigabit Ethernet I
Hard Disk: C:\Users\Public\Documents\Microsoft Hyper-V\Virtual H
Operating System: Will be installed at a later time

Bước 4: Chọn Media - DVD Drive - Capture I→ Action - Reset để reset máy ảo→ Bắt đầu quá trình cài đặt Vista→thao tác với máy ảo và hoàn tất việc cài đặt Hệ Điều hành

Windows Vista
Language to install: English
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
Copyright © 2006 Microsoft Corporation. All rights reserved.
Next

5- TÓM TẮT NỘI DUNG

- Lưu trữ dữ liệu trực tuyến (on-line): thiết bị lưu trữ được kết nối thường xuyên vào hệ thống thông tin
- Lưu trữ dữ liệu không trực tuyến
- Sao lưu toàn bộ dữ liệu sẽ được ghi ra thiết bị lưu trữ
- Quản lý phương tiện lưu trữ di động (removable media management)
- Sao lưu máy trạm (Workstation – backup).

6. CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày các lựa chọn khi Backup.

Câu 2: Trình bày mất mát dữ liệu do lỗi "vật lý" (mất mát vật lý)

Câu 3: Trình bày mất mát dữ liệu do lỗi "logic" (mất mát logic)

Câu 4: Nêu các yếu tố cần quan tâm đối với kỹ thuật khôi phục dữ liệu.

BÀI TẬP

Bài tập 1::**Backup và Restore database AD DS trên windows server 2008**
Yêu cầu: Cấu hình Backup và Restore win 2k8

Chuẩn bị: Một máy PC ài Windows server 2008 nâng cấp lên DC

Hướng dẫn làm bài

1.Cài đặt Windows Server Backup Feature

B1:Chọn Start → chọn Programs → chọn Administrative Tools → chọn Server Manager → chọn Features → chọn Add Features

B2:Trong cửa sổ "Select Features", chọn Windows Server Backup Features, chọnWindows Server Backup và Command-line Tools→ Next để tiếp tục→Install, để thực hiện quá trình cài đặt liên tục→Close.

2.Tạo một Scheduled Backup

B1: Chọn Start →Progams→ Administrative Tools →Windows Server Backup→Actions →Backup Schedule.

B2:Trong cửa sổ "Getting Started"→Next→Trong cửa sổ "Select backup configuration"→Custom → Next

B3:Trong cửa sổ "Specify backup time", chọn Once a day, chọn 10:30 am→Next.

B4:Trong cửa sổ "Select destination disk", chọn Show All Available Disks→Trong cửa sổ "Show All Available Disks", chọn Disk 1, chọn OK.

B5:Trong cửa sổ "Select destination disk", chọn Disk →Next→Trong cửa sổ "Windows Server Backup", chọn Yes → Next.

B6:Trong cửa sổ "Windows Server Backup", chọn Yes →Next→Trong cửa sổ "Confirmation", chọn Cancel tránh format ổ E→Trong cửa sổ "Summary", chọn Close

3.Thực hiện Backup AD

B1:Chọn Start → chọn Run→gõ CMD → chọn OK

B2:Gõ lệnh: wbadmin start systemstatebackup –backuptarget:f: →Sau đó nhấn phím y →nhấn phím Enter→ Quá trình backup diễn ra tầm 20 đến 30 phút→ Vào ổ F kiểm tra.

B3:Mở Active Directory Users and Computers, chọn menu View → Advanced Features→Click phải chuột vào OU IT → chọn Properties, chọn Tab Object, bỏ dấu check ở mụcProtect object from accidental deletion →chọn OK

B4:Click phải chuột vào OU IT → chọn Delete

4.Restore database AD DS

B1:Trên máy DC, chọn Start → chọn Command Prompt, Nhập bcdedit /set safeboot dsrepair, nhấn phím ENTER.

B2:Restart máy, sau đó nhấn F8, chọn Directory Services Restore Mode

B3:Restore dữ liệu system state→nhập shutdown -t 0 -r, nhấn phím ENTER. Máy tính sẽ Restart

B3:Logon với tài khoản Local Administrator→Start, nhấp chuột phải Command Prompt, chọn Run as administrator→tại Command prompt, Nhập lệnh : wbadmin get versions

Bài tập 2:: BACKUP- SHADOW COPY. Trên win2k2012

Yêu cầu: Cấu hình Shadow Copy

Chuẩn bị: 1 máy PC cài win 2012

Hướng dẫn làm bài

B1:Vào C →tạo folder Shadow → data.txt (thêm nội dung là: "123") → save lại. Sau đó Share folder Shadow.

B2: Phải chuột ổ C → Properties → tab Shadow copies (mặc định tính năng này bị disable) → Enable.

B3: Cấu hình thời gian mà Shadow Copy tự động nhân bản→Setting→torage Area: chọn nơi lưu trữ các bản sao→Để thiết lập thời gian → chọn schedule, mặc định Windows thiết lập 2 thời điểm:
+ 7h sáng hàng ngày: để copy các dữ liệu từ chiều hôm trước
+ 12h trưa: copy các thông tin phát sinh từ sáng.

B4: Kiểm tra→Mở Data.txt chỉnh sửa thành "456" → save lại →Mở tab Shadow Copies trong ổ C

B5: restore dữ liệu về thời điểm nào thì Properties Data.txt → Tab Previous version (tab này chỉ có khi enable tính năng Shadow)→ Restore.

Bài 4: CÀI ĐẶT VÀ QUẢN LÝ REMOTE ACCESS SERVICES (RAS) TRONG WINDOWS SERVER

Mã bài:MĐ 24-04

Thời gian: 6 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Đánh giá được những ứng dụng thường gặp của Remote Access Service;
- Đánh giá được thông lượng trên đường truyền;
- Cài đặt và cấu hình được mối nối kết nối Internet của RAS Server;
- Có khả năng tiếp nhận được các cuộc gọi ở xa
- Thực hiện các thao tác an toàn với máy tính.

II. NỘI DUNG CHÍNH

1.Những ứng dụng thường gặp của RAS

Ứng dụng của RAS

Sử dụng Remote Access Services như một phương tiện để cho phép người dùng đang ở xa quay số vào mạng công ty. Trong các tình huống như vậy, việc sử dụng Remote Access Services và quay số để kết nối cũng là một cách sử dụng khi không có các kết nối băng thông rộng trong các vùng đó.

2.Dự trù và những lưu ý về thông lượng đường truyền

Sự cố đường truyền

Nếu gặp phải sự cố trong thiết lập kết nối bằng modem, phải thực hiện trên máy khách hoặc máy chủ. Điều này rất dễ phát hiện vì nếu sự cố tồn tại trên máy chủ thì các máy khác quay số vào máy chủ đều không kết nối được, còn không như vậy thì vấn đề sẽ là do máy khách.

Trước khi quyết định vấn đề có thuộc về máy khách hay không, phải quan sát xem máy chủ có sử dụng nhiều đường điện thoại không. Nếu máy chủ sử dụng nhiều đường điện thoại thì nên thực hiện một số bài test để xem liệu máy khách khác có thể quay số và thiết lập một kết nối tới cùng đường điện thoại mà máy kia không thực hiện được.

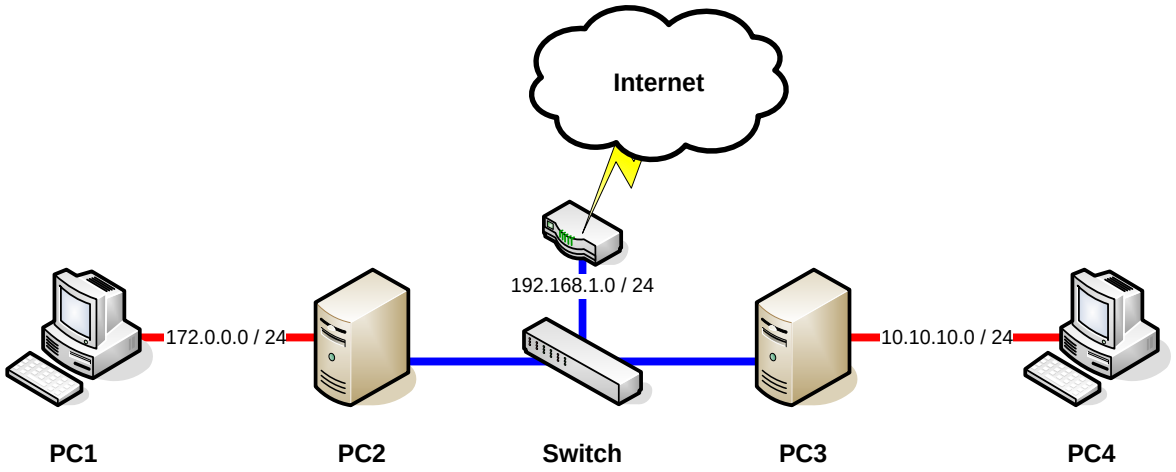
3.Các yêu cầu về phần cứng để thực hiện RAS

3.1 Chuẩn bị

+ Hai máy tính làm máy client cài windows XP hoặc windows server 2000 trở lên. Có ít nhất một card mạng LAN (RJ45)
+ Hai máy tính làm máy server cài windows server 2003. Có ít nhất hai card mạng LAN (RJ45)

+ Hai sợi cable bấm chéo (1-3, 2-6). Dùng để nối máy client với máy server.
+ Ba sợi cable bấm thẳng. Dùng để nối máy server với Switch và Switch với router ADSL
+ Một Switch.
+ Một router ADSL kết nối Internet
+ Một đĩa Windows Server 2003

3.2 Đấu nối các thiết bị theo mô hình sau



Đổi tên card mạng và cấu hình địa chỉ IP cho các máy như sau:

Máy	Đặc tính	PC1	PC2	PC3	PC4
Card LAN	IP Address	172.0.0.2	172.0.0.1	10.10.10.1	10.10.10.2
	Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Default gateway	172.0.0.1	N / A	N / A	10.10.10.1
	DNS	203.162.4.190 203.162.4.191	N / A	N / A	203.162.4.190 203.162.4.191
Card Internet	IP Address	N / A	192.168.1.2	192.168.1.3	N / A
	Subnet Mask	N / A	255.255.255.0	255.255.255.0	N / A
	Default gateway	N / A	192.168.1.1	192.168.1.1	N / A

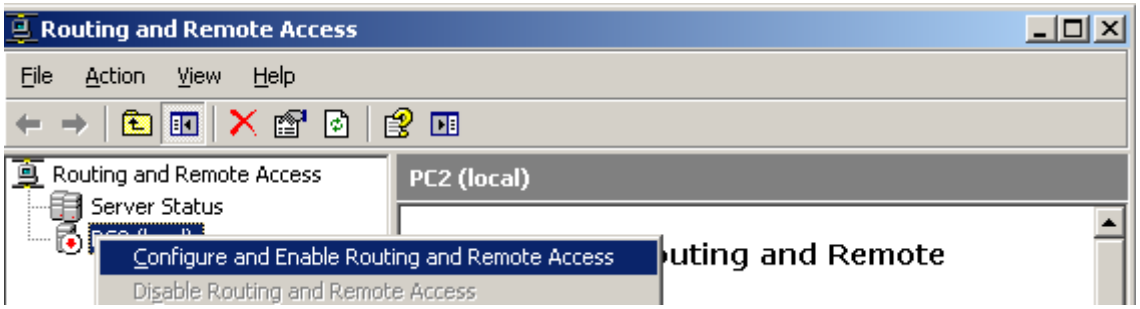
	Preferred DNS	N / A	203.162.4.190 203.162.4.191	203.162.4.190 203.162.4.191	N / A

Card Lan: Nối trực tiếp các cặp máy PC01 với PC02 và PC03 với PC04
Card Internet: Nối gián tiếp 2 máy PC02 & PC03 với nhau thông qua Switch
DNS của mỗi nhà cung cấp khác nhau bạn phải nhập đúng mới phân giải tên trên Internet được hoặc bạn có thể sài các DNS server miễn phí của **google (8.8.8.8 – 8.8.4.4)**

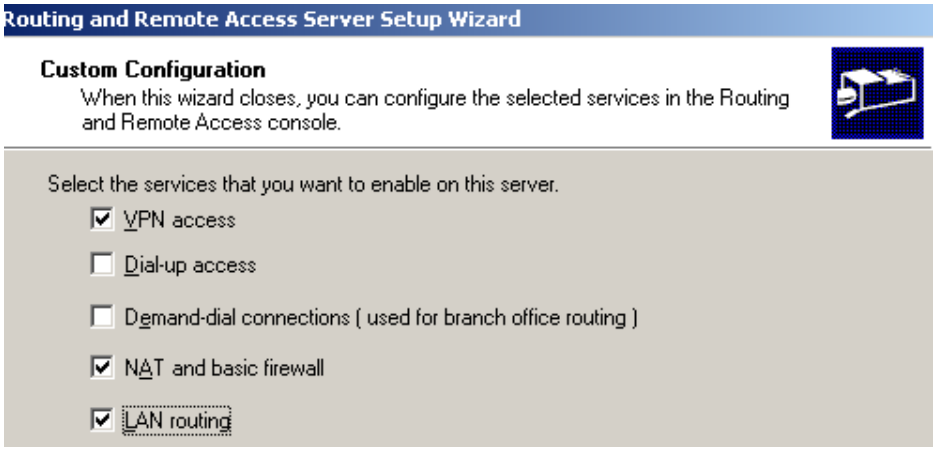
4.Tiếp nhận các cuộc gọi từ người dùng ở xa

Cài đặt, cấu hình cho các máy con ra internet

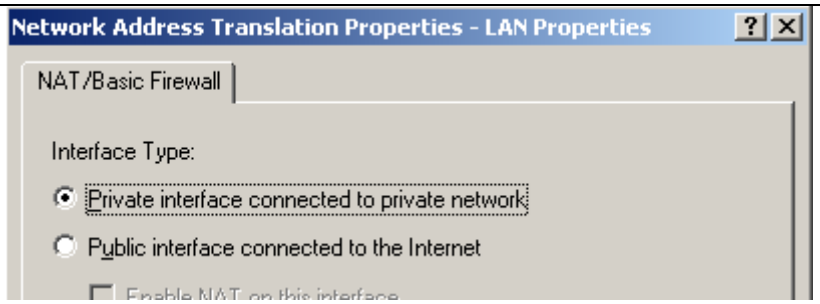
Bước 1: Vào Start → Programs →Administrative Tools → Routing and Remote Access, Tại cửa sổ Routing and Remote Access→ Nhấp phải chuột vào pc2(local)→ Configure and Enable Routing and Remote Access



Bước 2: Nhấn NEXT→ chọn Custom Configuration→Next→ check VPN access, NAT and basic firewal, LAN rounting→Next→ Finish


Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT and basic firewall
LAN routing

Bước 3: Chọn Public interface connected to the internet→OK→→ Card LAN→OK→ Check Private interface connected to private network→OK


Network Address Translation Properties - LAN Properties
NAT/Basic Firewall
Interface Type:
Private interface connected to private network
Public interface connected to the Internet

5.Kết nối một mạng VPN

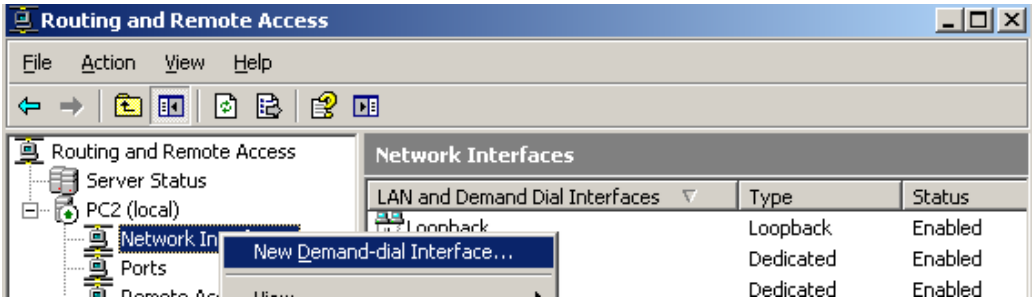
Mục tiêu: Có khả năng tiếp nhận được các cuộc gọi ở xa

5.1 Chuẩn bị

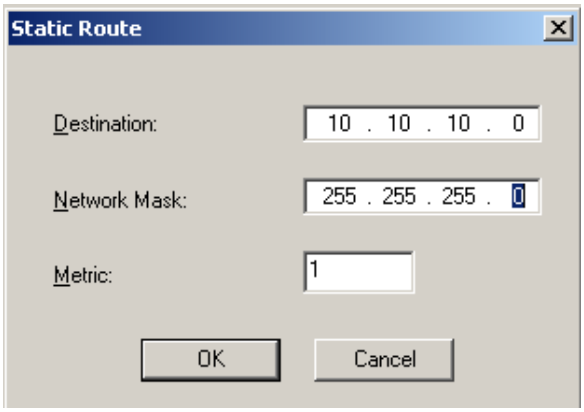
+ Để có thể truy cập mạng từ xa thông qua dịch vụ VPN ta cần một User cho phếp truy cập từ xa.
+ Trên máy pc2:Tạo User cho VPN client truy cập vào
+ 1 User…đặt tên mang 1
+ 1 User…đặt tên mang 2

5.2 Cài đặt

Bước 1:Cấp quyền đăng nhập→ Dial-in→ Allow access→OK→ Routing and Remote Access→ Network Interfaces→ New Demand-dial Interface →Next



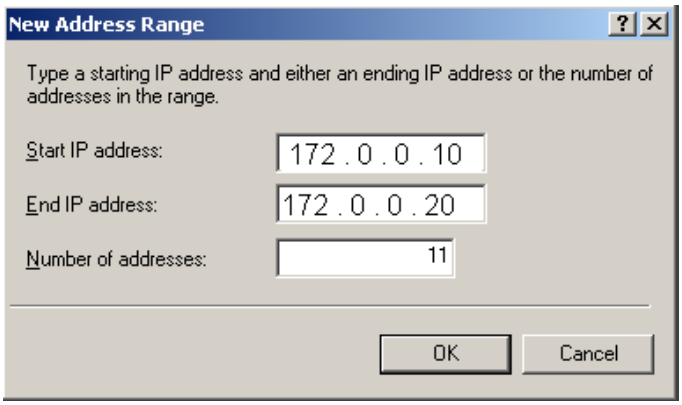
Bước 2: Interface Name→mang 2→Next→ Connect using virtual private networking (VPN)→Next→ Nhập IP card mạng Internet của mạng 2 (192.168.1.3)→Next



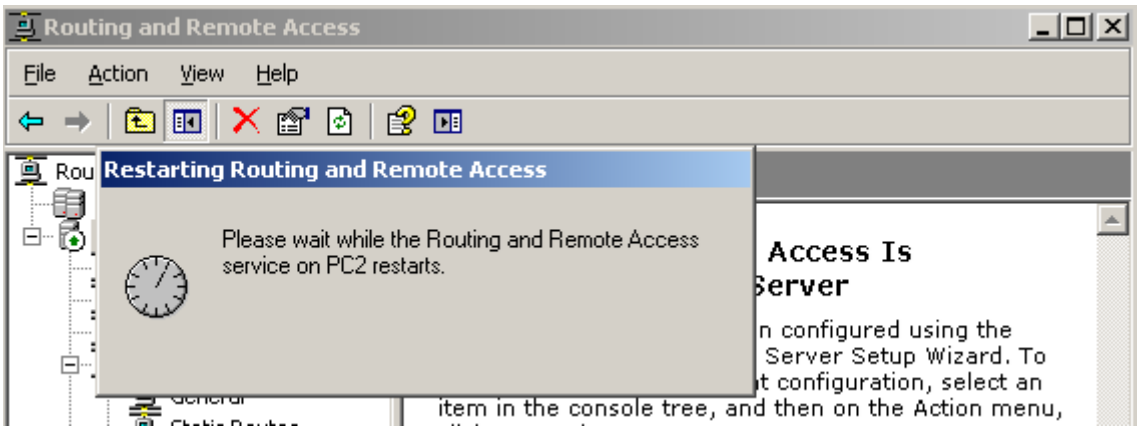
Destination: 10.10.10.0 (lớp mạng LAN cần đến)→ Network Mask:

255.255.255.0→ Metric: 1 (mặc định)→next→OK→ Dial Out Credentials→mang 2→next→ Finish

Bước 3: Routing and Remote Access→pc2→ Properties→ New Address Range nhập vào địa chỉ muốn cấp cho VPN client→ Start IP adress: 172.0.0.10→ End IP adress: 172.0.0.20→OK


New Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
172 . 0 . 0 . 10
End IP address:
172 . 0 . 0 . 20
Number of addresses:
11
OK
Cancel

Bước 4: Nhấp phải vào pc2(local) chọn All Tasks → Restart.



Trên máy pc3:

Làm tương tự như trên PC2 với các thông số sau:

Tạo User cho VPN client truy cập vào:

User name: mang2

Cấu hình cho VPN server:

Interface Name: mang1

Host name ỏ IP address: 192.168.1.2

Tại bản Static Route

Destination: 172.0.0.0 (Lớp IP mạng LAN của mạng 1)

Network Mask: 255.255.255.0

Metric: 1 (mặc định)

Tại bản Dial Out Credentials

User name: mang1 (User mà mạng 1 bạn đã Tạo)

Domain: (không cần nhập)

Password, Confirm password (password của user "mang1")

Address Range

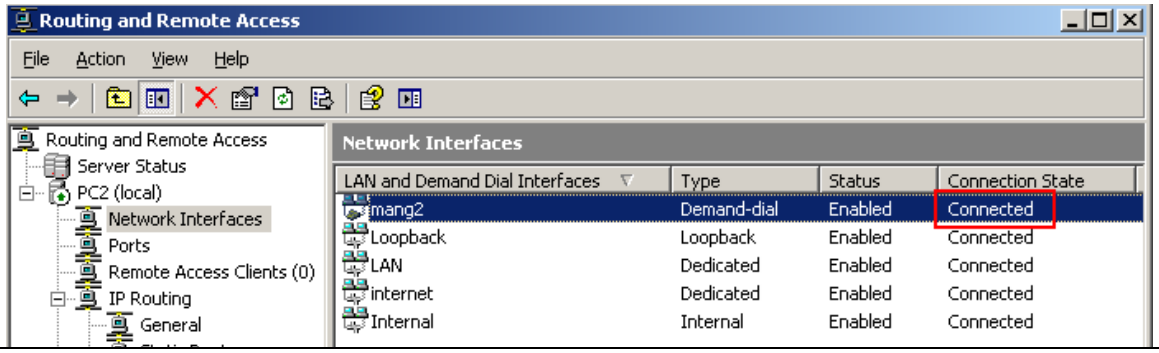
Start IP adress: 10.10.10.10

End IP adress: 10.10.10.20

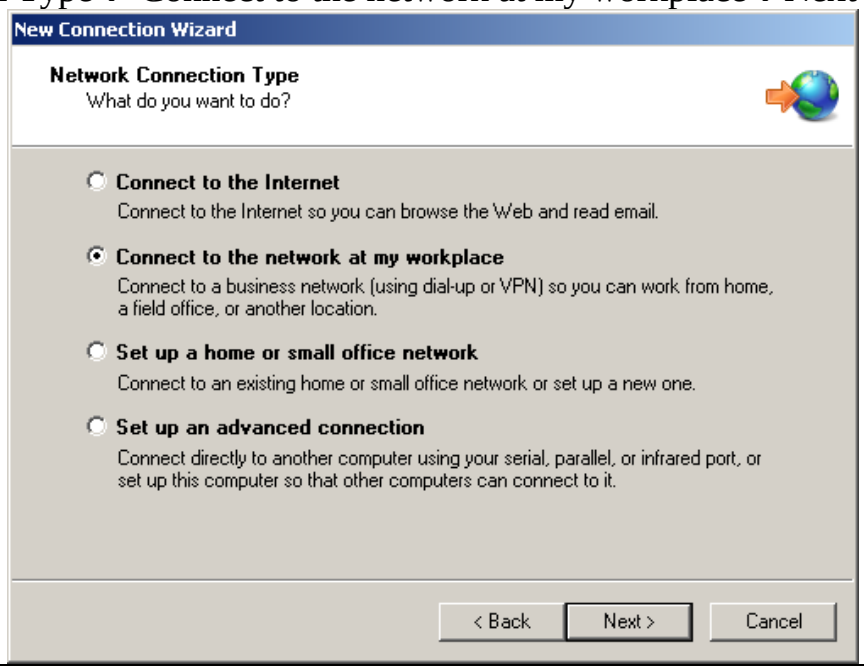
Lưu ý: Tên máy PC2(local) bây giờ là PC3(local) Sau khi hoàn tất phải Restart dịch vụ như trên PC2(local) (All Tasks → Restart)

5.3 Cấu hình

Bước 1: Trong cửa sổ Routing and Remote Access→ Nhấp trái chuột vào Network Interfaces→ Interfaces tên mang2→ Nhấn phải chuột lên Interface này chọn connect



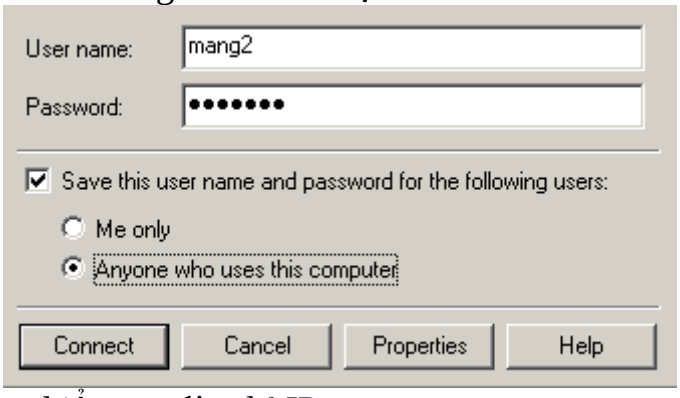
Bước 2: Network Connections→ File→ New Connection…→ Network Connection Type→ Connect to the network at my workplace→Next


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

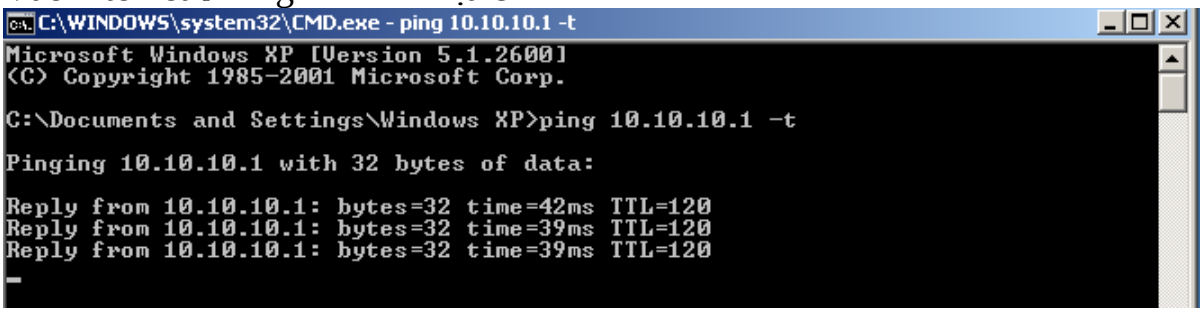
Bước 3: Network Connection→ Virtual Private Network connection→Next→ Connection Name→nhập mang 2→Next

New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
mang2

Bước 4: VPN Server Selection→ Host name or IP address nhập IP card mạng Internet của mạng 2 (192.168.1.3)→Next→ Network Connections→ Interface→ Connect→ mang2→user→mật khẩu



Vào internet→Ping kiểm tra địa chỉ IP


C:\WINDOWS\system32\CMD.exe - ping 10.10.10.1 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Windows XP>ping 10.10.10.1 -t
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=42ms TTL=120
Reply from 10.10.10.1: bytes=32 time=39ms TTL=120
Reply from 10.10.10.1: bytes=32 time=39ms TTL=120

Làm tương tự trên máy pc4.

6.TÓM TẮT NỘI DUNG

- Sử dụng dịch vụ Routing and Remote Access Service, hỗ trợ thông mạng 2 lớp mạng khác nhau.
- Dịch vụ RAS là dịch vụ được tích hợp vào hệ điều hành Windows 2003 server để hỗ trợ kết nối từ xa của các máy trạm vào hệ thống mạng.
- RAS trên windows 2003 cung cấp hai loại kết nối Dial-up Networking và Virtual Private Networking.
- Đặc điểm của routing and remote access cung cấp một số kỹ thuật như:
  + Network address translation (NAT)
  + Multiprotocol routing
  + Layer Two Tunneling Protocol (L2TP)

+ Internet Authentication Service (IAS)
+ Remote Access Policies (RAP).

7.CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

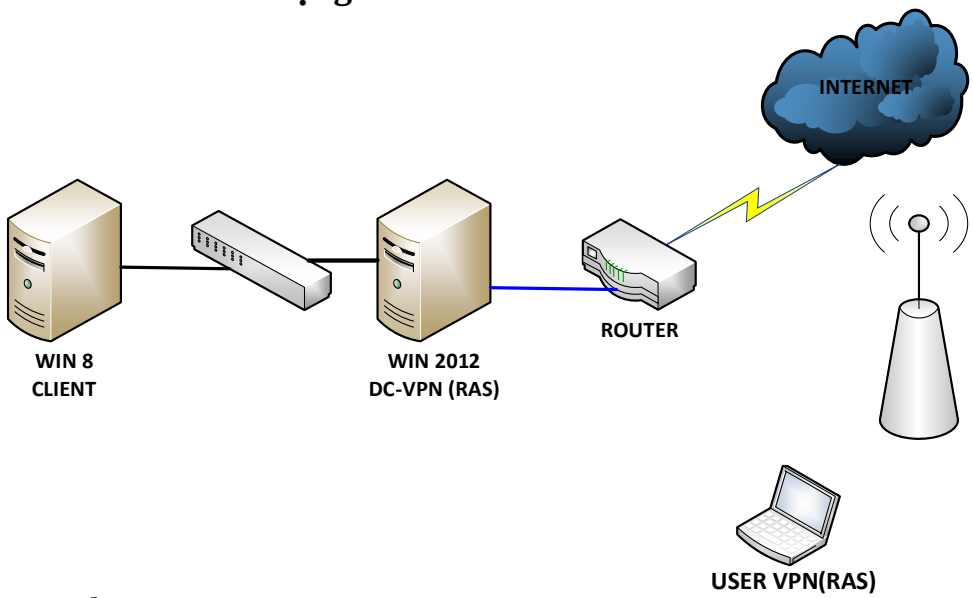
Câu 1: Trình bày khái quát về VPN (RAS)

Câu 2:Nêu các ưu khuyết điểm của RAS

Câu 3: Lập bảng so sánh intranet VPN(RAS) và extranet VPN(RAS)

BÀI TẬP

Bài tập 1: **Cho mô hình mạng**



Yêu cầu: **Triển khai VPN- RAS trên windows 2012**
Chuẩn bị:

- 1 máy Cài đặt win 2012→DC→VPN
- 1 máy cài win8
- 1 máy USER→VPN(RAS
- Tạo User cho VPN (RAS) client
- 1 Switch
- 1 router internet
- 3 sợi cáp bấm th ẳng

Hướng dẫn làm bài

1 Cài đặt dịch vụ VPN(RAS)

B1: Windows server 2012 triển khai service VPN chúng ta sẽ tiến hành Joind Domain. Mục đích join domain để các user ngoài internet khi VPN sẽ yêu cầu chứng thực bằng user trong Domain

B2: Restart lại server và login bằng user administrator của Domain

B3: Để cài dịch vụ VPN → Server Manager → Add roles & Features

B4: Chọn và cài đặt role "Remote Access"→ DirectAccess and VPN (RAS) →Close

2. Cấu hình VPN (RAS)

B1: Tools → Routing and Remote Access→ Run the Remote Access setup để cấu hình tính năng VPN

B2: Direct Access→ enable Routing and Remote access→ Custom Configuration

B3: VPN →LAN → Right click trên VPN server→Kết n ối VPN (RAS)

Bài tập 2: Routing and Remote Access, Lan routing trên Server 2012 để giúp máy tính biến thành router ảo.

Yêu cầu:
Chuẩn bị:

- 1 máy Cài đặt win 2012→DC→VPN
- 1 máy cài win8
- 1 máy USER→VPN(RAS
- Tạo User cho VPN (RAS) client
- 1 Switch
- 1 router internet
- 3 sợi cáp bấm thẳng

Hướng dẫn làm bài

B1: Routing and Remote Access trên Server 2012 làm như sau: Run (Ctrl + R) → rrasmgmt.msc

B2: Mặc định tính năng bị disable→Configure and Enable Routing and Remote Access→ Next

B3: Custom Configuration→ check Lan routing→ Finish.

B4: Static routes → New static route→ All Tasks → Restart

B5: Static Routes → Show IP Routing Table→ General → New Routing Protocol.

B6: RIP Version 2 for Internet Protocol→ RIP → New Interface

BÀI 5:GROUP POLICY OBJECT
Mã bài:MĐ 24-05

Thời gian: 11 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày được chức năng của Group policy;
- Tạo và quản lý các đối tượng trong GPO.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CH ÍNH

1.Giới thiệu Group policy

Triển khai ứng dụng Group policy

Triển khai phần mềm ứng dụng: có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (package), đặt nó lên Server, rồi dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.

Gán các quyền hệ thống cho người dùng: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt máy server, đổi giờ hệ thống hay backup dữ liệu…

Giới hạn những ứng dụng mà người dùng được phép thi hành: chúng ta có thể kiểm soát

Máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: Outlook Express, Word hay Internet Explorer.

Kiểm soát các thiết lập hệ thống: bạn có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.

Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy: trong hệ Windows Server 2003 thì hỗ trợ cả bốn sự kiện này được kích hoạt (trigger) một kịch bản (script). Có thể dùng các GPO để kiểm soát những kịch bản nào đang chạy.

Đơn giản hóa và hạn chế các chương trình: bạn có thể dùng GPO để gỡ bỏ nhiều tính năng khỏi Internet Explorer, Windows Explorer và những chương trình khác.

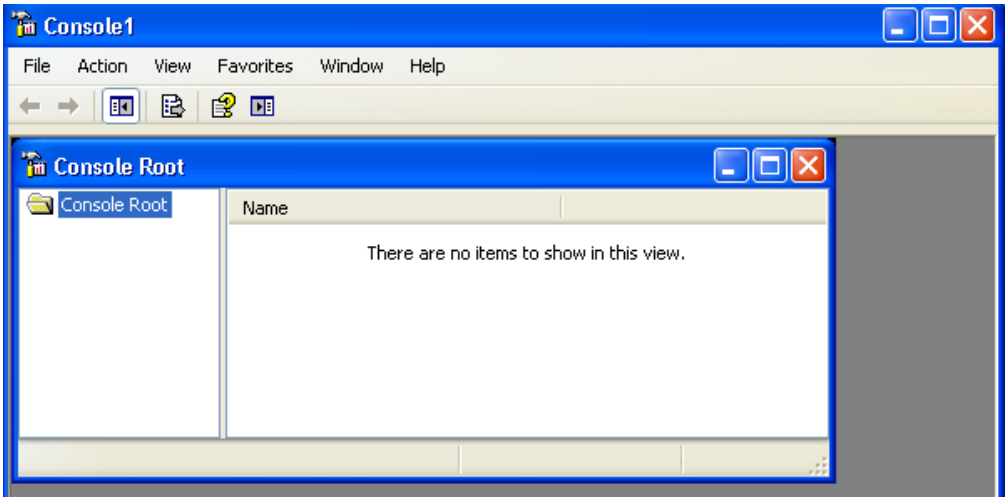
2.Tạo và tổ chức các đối tượng trong Group policy

Mục tiêu: *Tạo và quản lý các đối tượng trong GPO*

Tạo Group Policy trên Local Computer. Để tạo một GPO local, chúng ta phải được logon như là một thành viên Administrator có thể truy xuất Group Policy Object Editor từ Administrator Tools hay qua một snap-in MMC

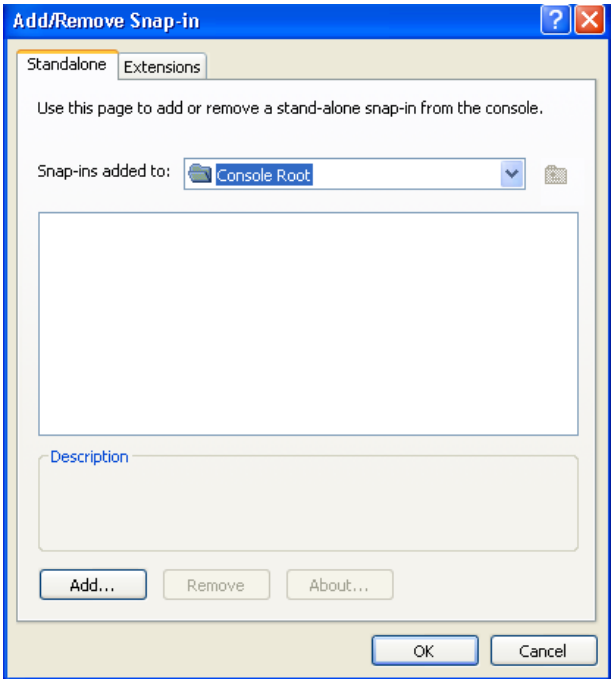
Cài đặt một policy với những thiết lập local

Bước 1:Start → Run và nhập vào mmc →OK

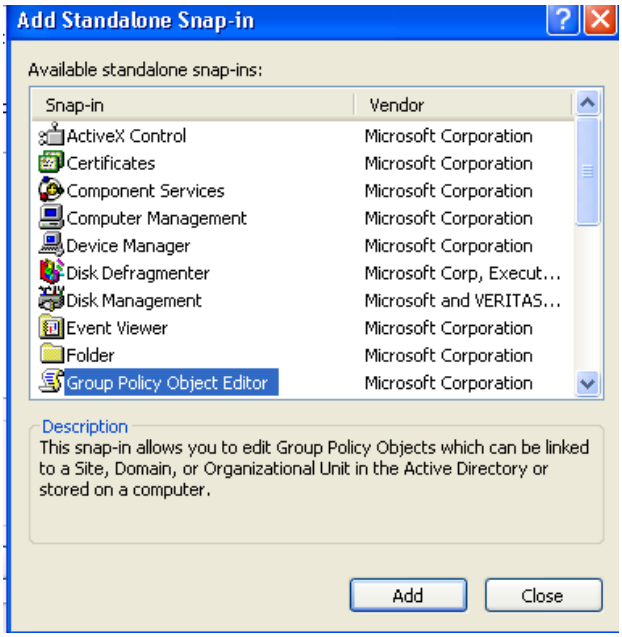


Hình 5-1: màn hình console

Bước 2:Vào menu Files → Add/Remove Snap-in…→Add Group Policy Object Editor

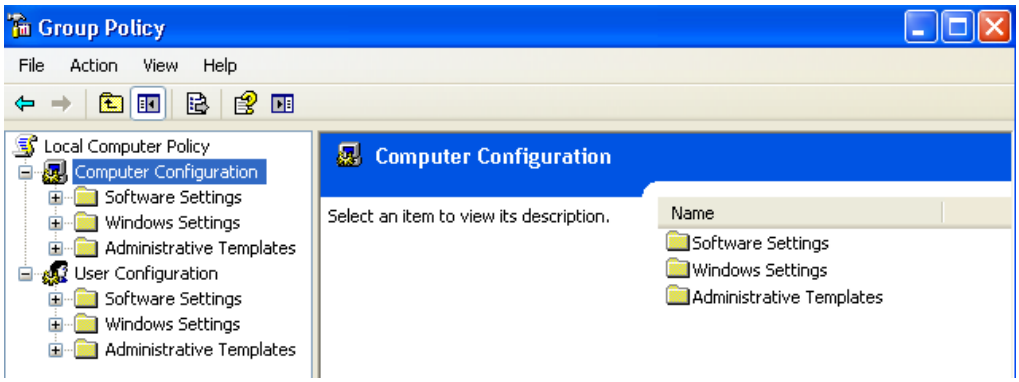


Hình 5-2:màn hình add Snap-in



Hình 5-3: màn hình tùy chọn Open Group Policy

- Mở Group Policy Object Editor.
- Trong conse nhấp đúp vào policy settings in the details pane.
- Trong details pane nhấp đúp vào policy setting chọn Properties dialog box, và thay đổi policy setting.



Hình 5-4: màn hình tạo Group Policy

3.Thiết lập các chính sách trên Domain Controller

Mục tiêu: *Xem và tạo các chính sách trên miền*

3.1 Xem chính sách cục bộ của một máy tính ở xa

Để xem một chính sách cục bộ trên các máy tính khác trong miền, phải có quyền quản trị trên máy đó hoặc quản trị miền. Có thể dùng lệnh GPEDIT.MSC /gpcomputer:machinename.

Ví dụ:muốn xem chính sách trên máy PCO1 gõ lệnh GPEDIT.MSC /gpcomputer: PCO1. Chú ý là không thể dùng cách này để thiết lập các chính sách nhóm ở máy tính ở xa, do tính chất bảo mật Microsoft không cho phép ở xa thiết lập các chính sách nhóm

3.2 Tạo các chính sách trên miền

Chúng ta dùng snap-in Group Policy trong Active Directory User and Computer hoặc gọi trực tiếp tiện ích Group Policy Object Editor từ dòng lệnh trên máy Domain Controller để tạo ra các chính sách nhóm cho miền. Nếu mở Group Policy từ Active Directory User and Computer thì trong khung cửa sổ chính của chương trình nhấp chuột phải vào biểu tượng tên miền (trong ví dụ này là netclass.edu.vn), chọn Properties. Trong hộp thoại xuất hiện chọn Tab Group Policy.

3.3 Bài tập thực hành

Yêu cầu

- Làm mất control panel đối với cac user thuộc group KeToan
- Làm mất biểu tượng Rycecle Bin trên Desktop đối với cac user thuộc group NhanSu
- Làm ẩn biểu tượng My Network Place cho các users nằm trong OU Nhatnghe

Chuẩn bị:

- Khởi động máy chọn windows server 2003 đã nâng cấp lên Domain Controller
- Bỏ giới hạn password (Domain Security Policy → Account Policies → Password Policy)
- Tạo OU tên: "NhatNghe"
- Trong OU NhatNghe, tạo 2 OU: "Nhansu", và "KeToan"
- Trong OU KeToan tạo 2 user: "KT1", "KT2"
- Trong OU NhanSu tạo 2 user: "NS1", "NS2"
- Cho group Users quyền Allow Logon Locally (Domain Controller Security Policy →Local Policy → User Right Assignment → Allow log on locally→ add group users vào→Gpupdate /Force

Thực hiện

Tạo group policy

Làm mất control panel đối với cac user thuộc group KeToan

Bước 1: Logon Administrator → vào Active Directory User And Computer → click phải chuột lên OU KeToan → Properties → chọn tab Group Policy → new →đặt tên "mat control panel" → Edit

Bước 2: Chọn User Configuration → Administrative Templates → Control Panel → click phải chuột trên Prohibit Access To The Control Panel (ở cửa sổ bên phải) → Properties → Enable → Apply → OK → close cửa sổ Group Policy → OK

Logoff administrator → logon KT1→ Vào start → setting (control panel đã bị mất)

Làm mất biểu tượng Rycecle Bin trên Desktop đối với cac user thuộc group NhanSu

Bước 1: Logoff KT1 → Logon Administrator → Vào Active Directory User And Computer → click phải chuột lên OU NhanSu → Properties → chọn Tab Group Policy → New →đặt tên "mat Rycecle Bin" → Edit

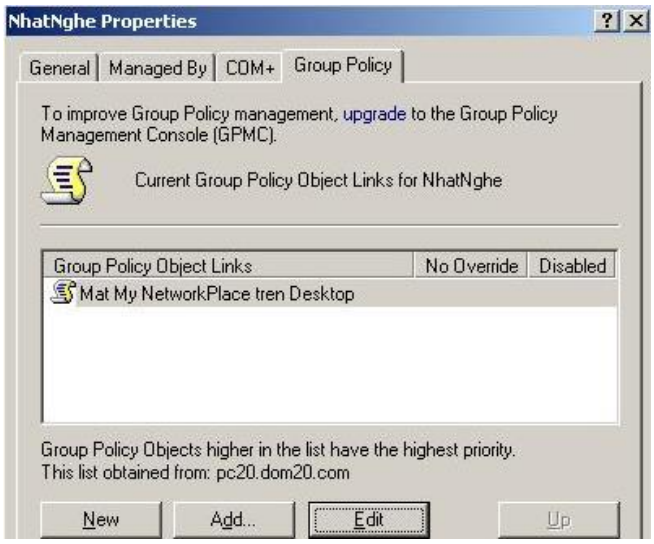
Bước 2: Chọn user configuration → administrative templates → Desktop → click phải chuột trên Remove Recycle Bin Icon From Desktop ở cửa sổ bên phải) → Properties → Enable → Apply → OK → close cửa sổ group policy →

OK

Cập nhật → Gpupdate /Force→ Logon NS1 , nhận xét thấy biểu tượng Recycle Bin đã mất trên màn hình desktop

Làm ẩn biểu tượng My Network Place cho các users nằm trong OU Nhatnghe

Bước 1: Logon Administrator → Vào Active Directory User And Computer → click phải chuột lên OU Nhatnghe→ Properties → chọn Tab Group Policy → New →đặt tên "mat My Network Place trên desktop" → Edit



Bước 2: Chọn User Configuration → Administrative Templates → Desktop → click phải chuột trên Hide My Network Place icon on desktop (ở cửa sổ bên phải) → Properties → Enable → Apply → OK → close cửa sổ group policy → OK

Cập nhật → Gpupdate /Force→ Logon KT1, nhận xét thấy biểu tượng My Network Place và Control Panel đã bị mất

4.Sử dụng GPO để triển khai Ms office

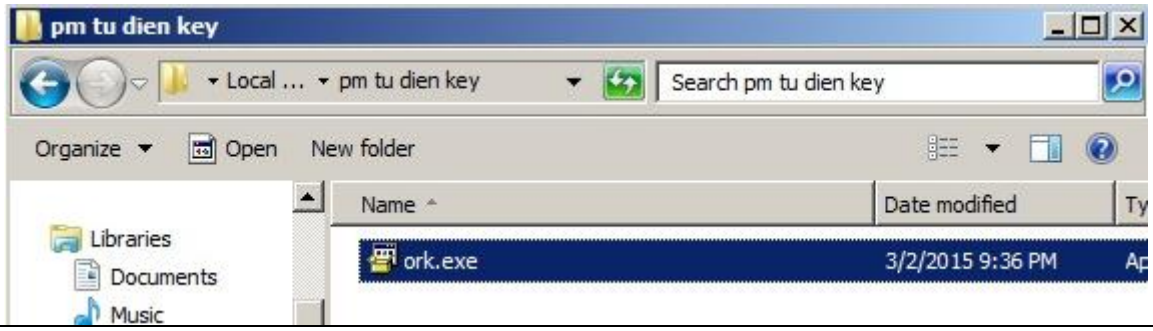
Mục tiêu:Cài đặt, cấu hình Msoffice trên GPO
Yêu cầu: Cài đặt MS office trên nền GPO

Chuẩn bị

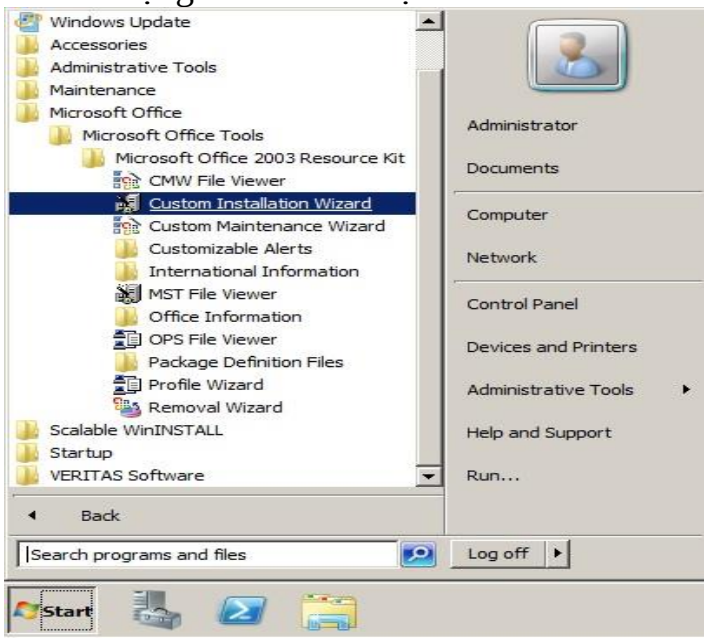
- Cấu hình domain
- Tắt firewall
- Cấu hình mạng thông nhau
- Share thư mục Office full quyền

Thực hiện

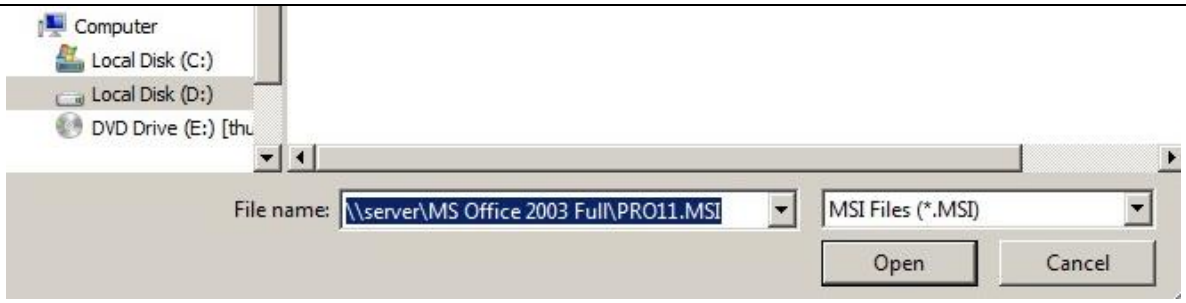
Bước 1: Cài đặt→ Chọn I accept …. → Next→ Typical Install → Next→ Install→OK



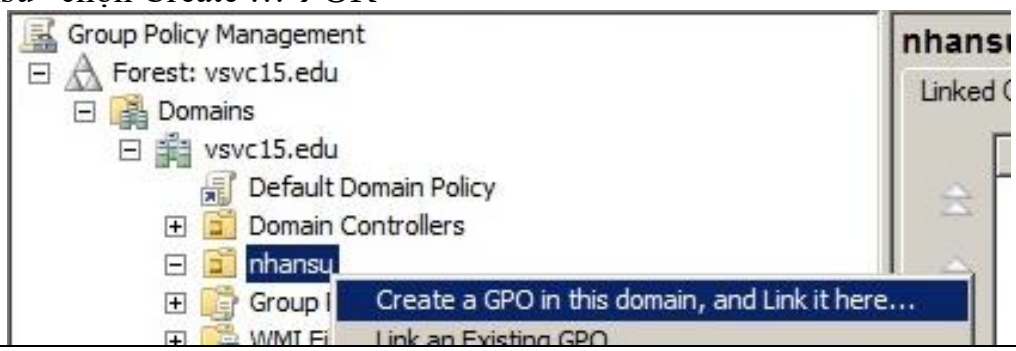
Bước 2: Vào Start khởi động file vừa cài đặt custom installation wizard



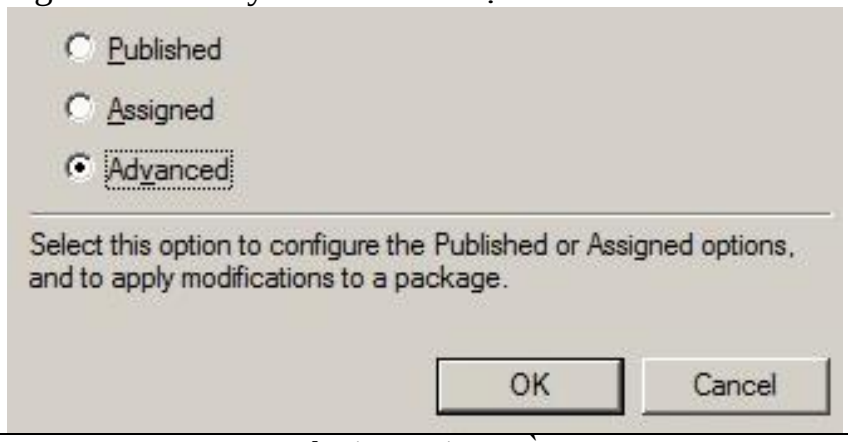
Bước 3: Chọn Next→\\tên máy server \ thư mục share\file.msi →Next→Next→Next→ Organization name: đặt tên tùy ý → Next



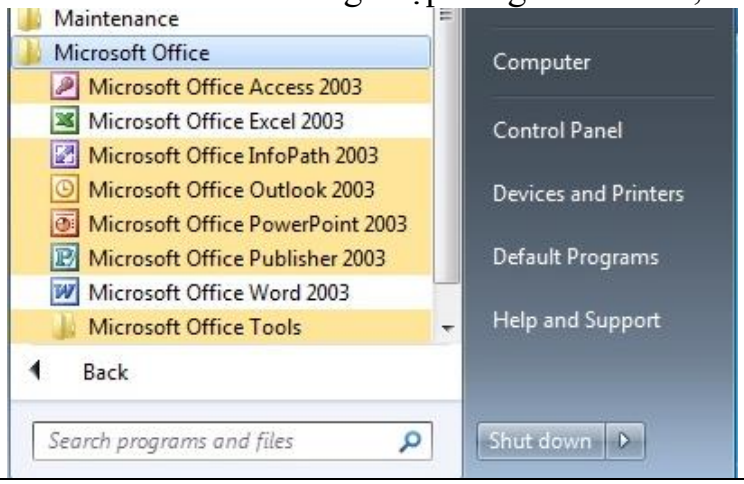
Bước 4: Cấu hình cho OU "nhansu"
Vào Start → chọn Group policy managerment → click phải chuột lên OU "nhansu" chọn Create …→OK



Bước 5: Click phải chuột lên tên vừa tạo → Edit→ Chọn User Configuretion → Polices → Software Setting → click phải chuột lên Software Installtion → new → Package→: \\tên máy server \ thư mục share\file.msi→OK



Bước 6: GPUPDATE /FORCE→ đăng nhập bằng user "ns1",



Bài tập 2::Fine-Grained Password Policies In Windows Server 2008

Yêu cầu:

Câu 1: THIẾT LẬP CÁC CHÍNH SÁCH HỆ THỐNG

- Mật khẩu đơn giản, tối thiểu 4 ký tự.
- Mật khẩu có thể thay đổi bất cứ lúc nào và bắt buộc phải thay đổi sau mỗi 14 ngày.
- Tài khoản sẽ bị khoá 2 giờ sau 3 lần đăng nhập không thành công

Câu 2: TẠO OU,GROUP,USER

- Có 4 phòng ban (ban Giám Đốc, Phòng Kế Toán, Phòng Nhân sự, Phòng kỹ thuật), mỗi phòng ban có tối thiểu là 3 User sử dụng máy tính.
- Tạo tập tin thongtin.doc trong ổ đĩa D có các thông tin liên quan đến các User,OU,group.

Các thuộc tính cho các User như sau:

- Giám đốc, phó giám đốc, trưởng phòng phải thay đổi mật khẩu lần đầu đăng nhập
- Các nhân viên không được phép thay đổi mật khẩu.
- Thời gian đăng nhập vào hệ thống của Giám đốc, phó giám đốc, trưởng phòng từ 8h- >20h mỗi ngày.
- Thời gian đăng nhập vào hệ thống của các thành viên còn lại từ 8h→12h và 14h → 18h vào các ngày từ thứ 2 → thứ 7.

Câu 3:TẠO THƯ MỤC VÀ PHÂN QUYỀN,QUOTA

- Mỗi người có một thư mục riêng trên máy chủ, Chỉ có Administrator và User đó có toàn quyền trên thư mục này, Thư mục này tự động ánh xạ về làm ổ đĩa W mỗi khi User đăng nhập vào hệ thống.
- Thiết lập Quota cho Giám đốc, phó giám đốc, trưởng phòng là 50Mb, Nhân viên là 20Mb
- Mỗi phòng ban có một thư mục riêng dùng để trao đổi dữ liệu với nhau. Chỉ có Administrator và trưởng phòng có toàn quyền trên thư mục này, những User khác trong phòng ban chỉ có quyền xem và ghi dư liệu lên thư mục này nhưng không được phép xóa sửa nội dung bên trong .Những User thuộc nhóm khác không có quyền mở thư mục này. Thư mục này tự động ánh xạ về làm ổ đĩa Z mỗi khi User đăng nhập vào hệ thống.
- Tạo tập tin **thongtinthumuc.doc** trong ổ đĩa D có các thông tin thư mục, quyền hạn truy cập thư mục của User, nhóm,OU.

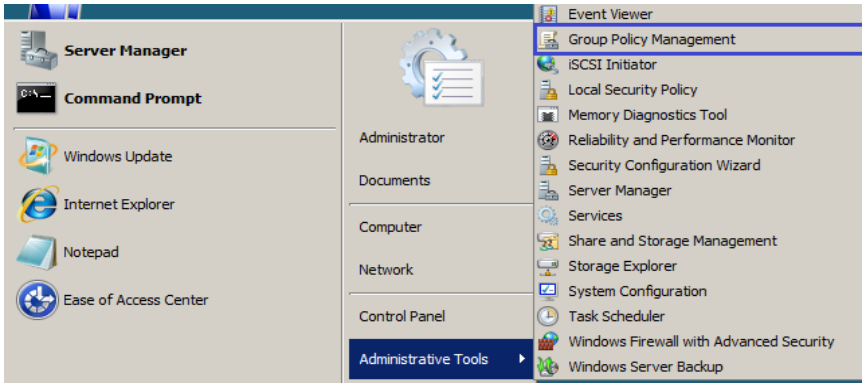
Chuẩn bị:

- 1 máy PC cài đặt win2k8 nâng cấp lên domain controller
- 1 máy PC cài đặt win7
- 1 sợi cáp thẳng nếu cắm qua switch
- 1 sợi cáp chéo nếu cắm PC→PC

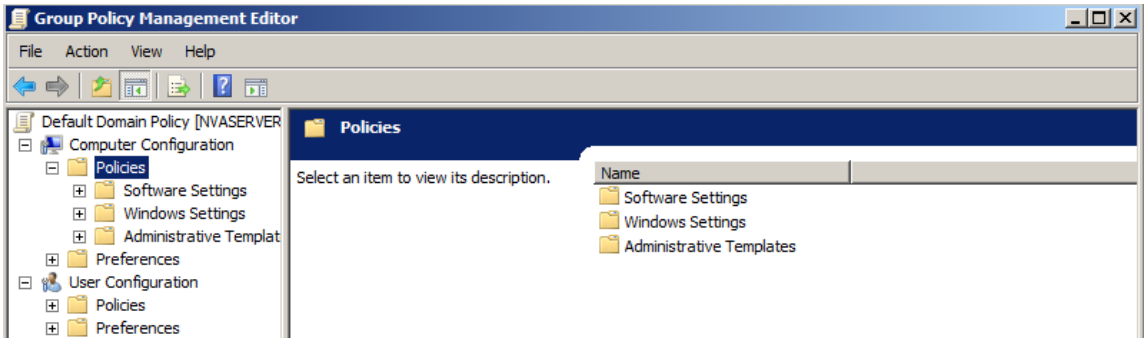
Thực hiện

Câu 1: THIẾT LẬP CÁC CHÍNH SÁCH HỆ THỐNG

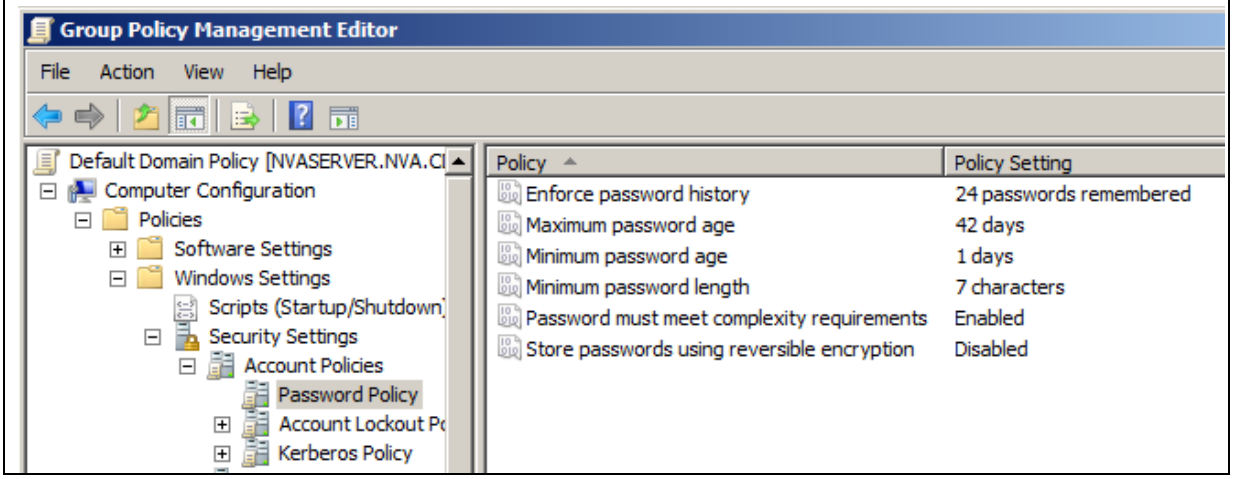
Bước 1: Vào Start → Administrative Tools → Group Policy Management



Bước 2: Click – Phải vào Default Domain Policy → Chọn Edit → Double – Click vào Policies

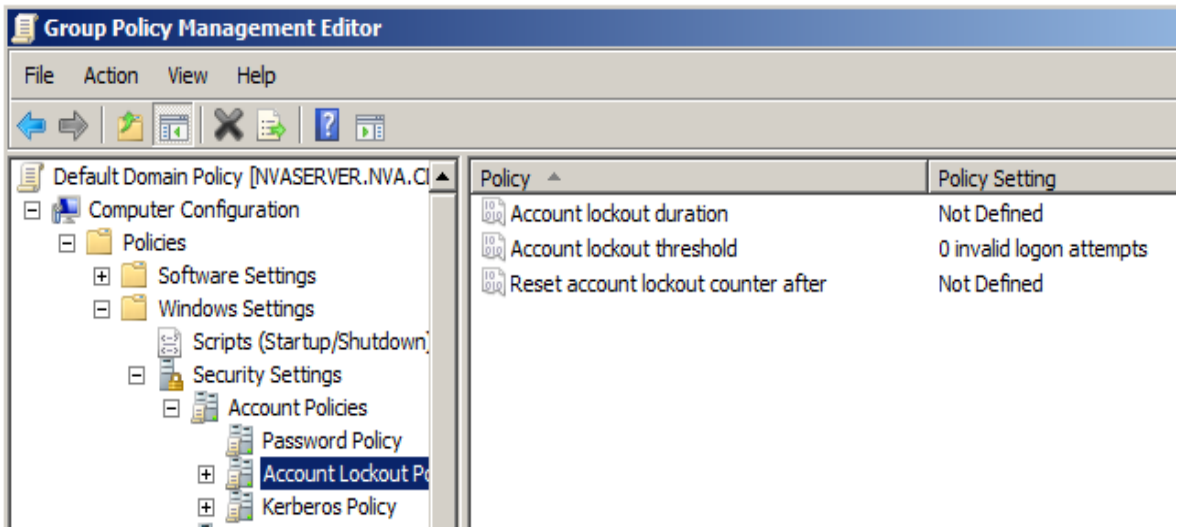


Bước 3: Double – Click vào Windows Settings→ Double – Click vào Security Settings→ Double – Click vào Password Policy



Enabled sang Disabled → OK

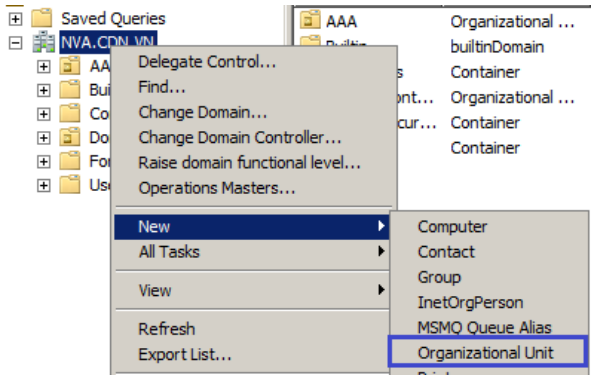
Bước 4 :Double – Click vào Account Lockout Policy chọn dòng Account lockout duration



Account will lock out after : Ta cho 3 invalid logon attempts (Đăng nhập quá 3 lần sẽ bị khóa)

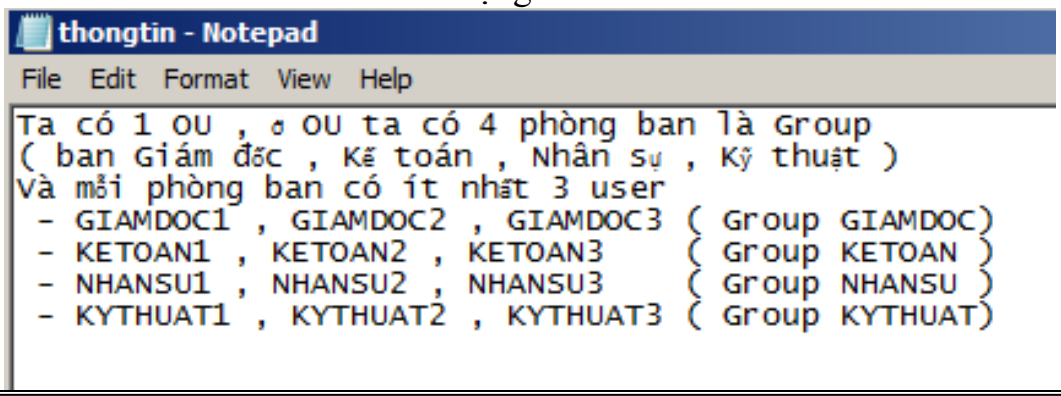
Câu 2: TẠO OU,GROUP,USER

Bước 1: : tạo OU Click – Phải domain NVA.CDN.VN → New → Organizational Unit

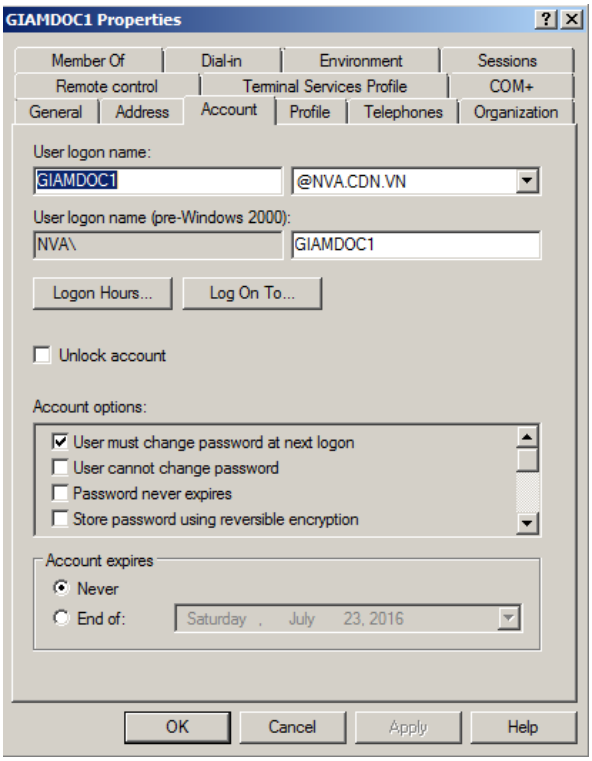


Đặt tên cho OU , VD : NVA → OK

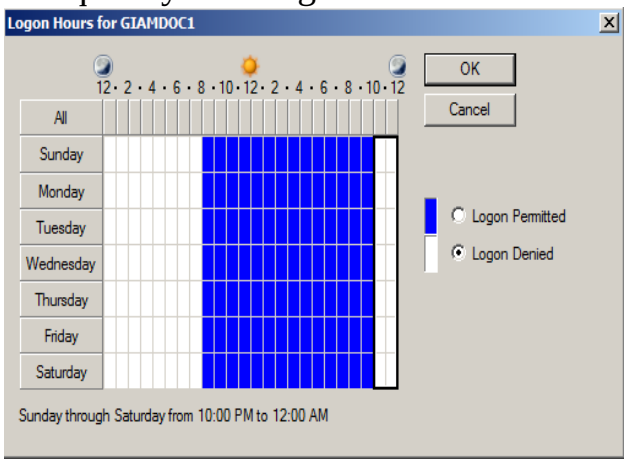
Bước 2: Tạo 1 tập tin thongtin.doc trong ổ đĩa D , Click – Phải chọn New → Text Document → Save as… dưới dạng đuôi .doc


thongtin - Notepad
File Edit Format View Help
Ta có 1 OU , ở OU ta có 4 phòng ban là Group
(ban Giám đốc , Kế toán , Nhân sự , Kỹ thuật)
Và mỗi phòng ban có ít nhất 3 user
- GIAMDOC1 , GIAMDOC2 , GIAMDOC3 (Group GIAMDOC)
- KETOAN1 , KETOAN2 , KETOAN3 (Group KETOAN)
- NHANSU1 , NHANSU2 , NHANSU3 (Group NHANSU)
- KYTHUAT1 , KYTHUAT2 , KYTHUAT3 (Group KYTHUAT)

Bước 3 :Quyền thay đổi mật khẩu→ Properties→ Account → ở phần Account options → tích chọn User must change password at next logon

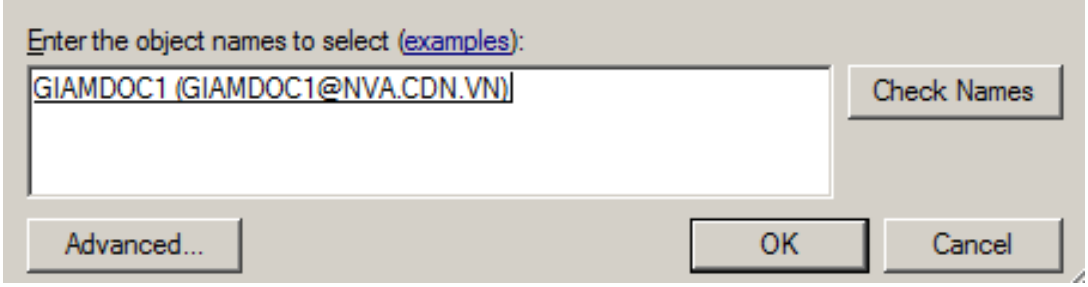


Bước 4: Thời gian ban quản lý→Thời gian nhân viên



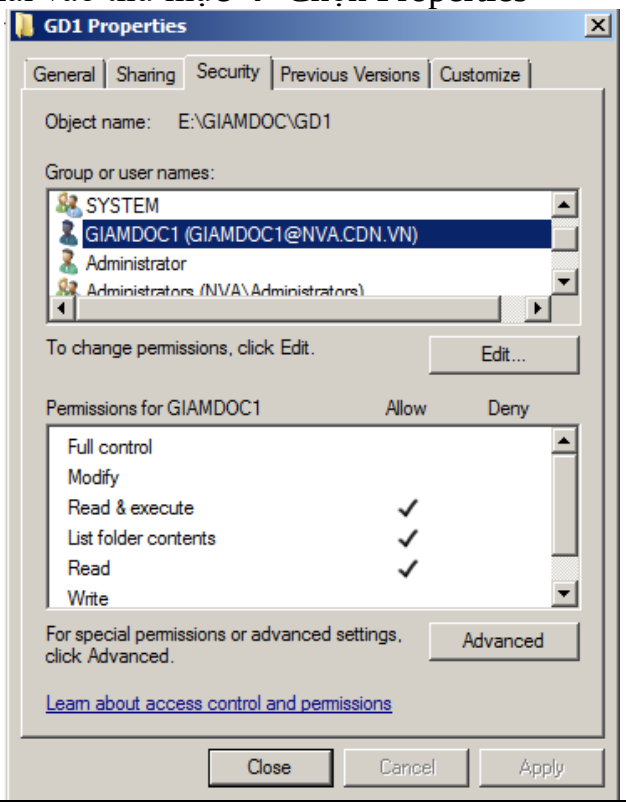
Câu 3:TẠO THƯ MỤC VÀ PHÂN QUYỀN,QUOTA

Bước 1: Click – Phải vào thư mực →Properties→ Share…→ Find (tìm) đến user cần sử dụng thư mục đó

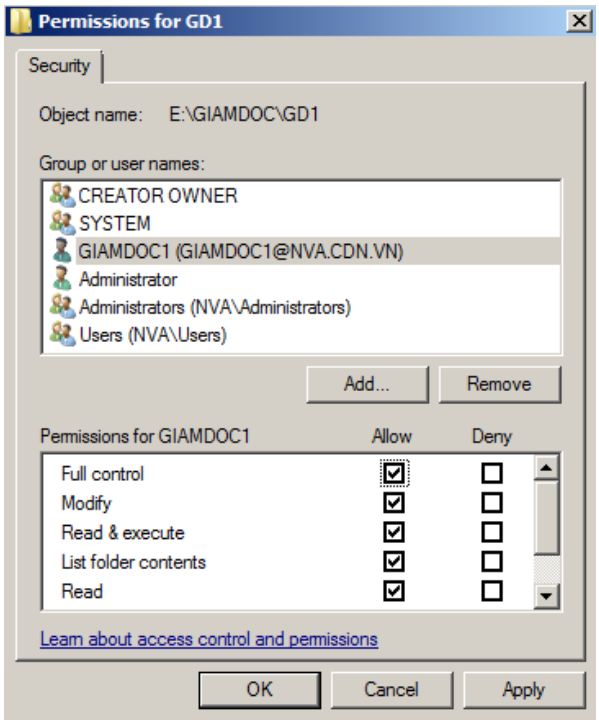


Check Names → Share → End

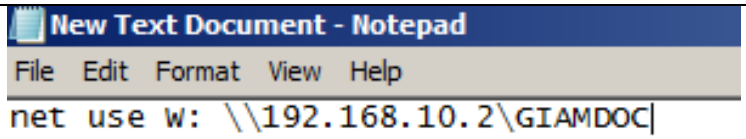
Bước 2: Click – Phải vào thư mục → Chọn Properties



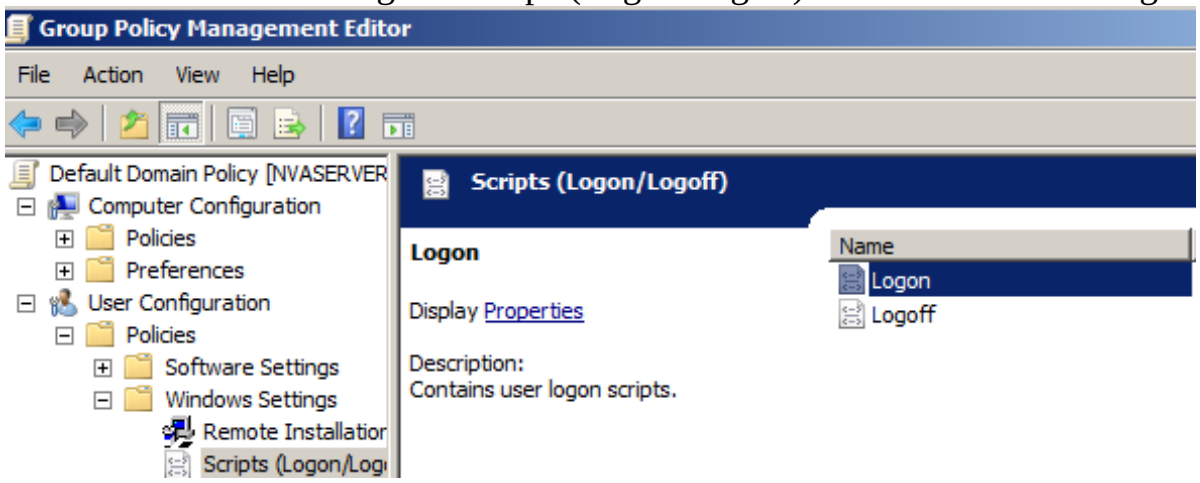
Bước 3: Tại tabSecurity → Chọn User và phân quyền Full control → OK (Các user khác tương tự)



Bước 4: : Ánh xạ ổ đĩa mỗi khi đăng nhập user →tạo 1 File Notepad → gõ lệnh net use w: \\192.168.10.2\GIAMDOC (net use w: \\server\thư mục share → Save as… bằng đuôi .bat.

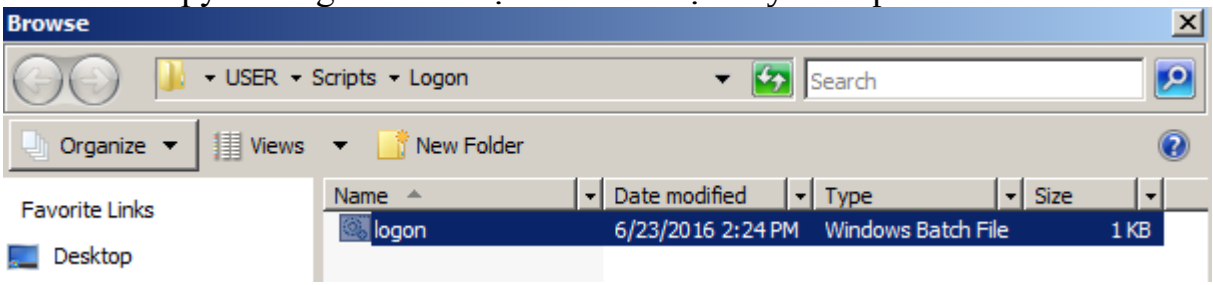


Bước 5: Windows Settings → Scripts(Logon/Logoff) → Double – Click Logon

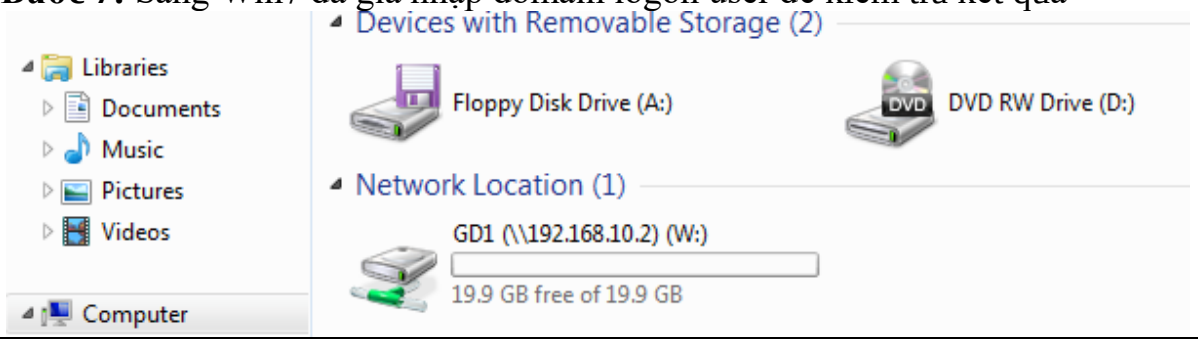


Add…→ Browse…

Bước 6: Copy file logon.bat đã tạo vào thư mục này rồi Open → OK



Bước 7: Sang Win7 đã gia nhập domain logon user để kiểm tra kết quả



5- TÓM TẮT NỘI DUNG

- Group Policy là tập các thiết lập cấu hình cho computer và user.
- Xác định cách thức để các chương trình, tài nguyên mạng và hệ điều hành làm việc với người dùng và máy tính trong 1 tổ chức. Group policy có thể thiết lập trên máy tính, site, domain, và OU.
- Sử dụng GPO để triển khai Ms office
- Thực hành cài đặt, cấu hình Group policy

6- CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày các chức năng của Group Policy.

Cầu 2: Trình bày các công cụ Group Policy (GP) trên Windows Server 2008

Câu 3: Trình bày các tính năng Windows Settings trong GROUP POLICY PREFERENCES Server 2008

Câu 4: Trình bày các tính năng Control Panel Settings trong GROUP POLICY PREFERENCES Server 2008

BÀI TẬP

Bài tập 1: Deploying Policies for Windows Firewall with Advanced Security win2k8

Yêu cầu:

- Thiết lập các Inbound and Outbound firewall rule
- Tạo các Group Policy Object (GPO) cấu hình tường lửa để triển khai cho hàng loạt máy tính
- Tạo các Isolation rule để chỉ định máy tính nào bị cô lập với các máy tính khác dựa trên các thành viên trong cơ sở hạ tầng Active Directory
- Tạo các Connection security rules để cách ly các máy server

Chuẩn bị

- Một máy Windows Server 2008, đã nâng cấp thành Domain Controller (DC)
- Hai máy Domain member
- Một máy Windows Server 2008, đã join domain
- Một máy Windows Vista, đã join domain
- Thiết lập IP

Interface	Parameter	Windows Vista (CLIENT)	Domain Controller (DC)	Windows 2008 (MBRSRV)
Lan	IP Add.	192.168.15.116 / 24	192.168.15.17 / 24	192.168.15.118 / 24
	D. Gateway	Không	Không	Không
	P. DNS	192.168.15.17	192.168.15.17	192.168.15.17

Hướng dẫn làm bài

1.Cấu hình MBRSRV thành Telnet Server và cài đặt feature Group Policy Management (thực hiện trên MBRSRV)

B1: Click phải Computer → Manage→ Click phải Features →Add Features

B2: Hộp thoại Select Features →Group Policy Management và Telnet Server →Next→Confirm Installation Selections →Install

B3: Hộp thoại Installation Results → Close→Start →Programs →Administrative Tools →Services→Click phải Telnet →Properties

B4: Hộp thoại Telnet Properties → chọn Automatic → Apply→Telnet Properties → chọn Start →Apply →OK

2.Cấu hình CLIENT thành Telnet Client (thực hiện trên CLIENT)

B1: Start →Settings →Control Panel→Control Panel → Click phải Programs and Features → Open

B2: Programs and Features → Chọn Turn Windows features on or off→Windows features → Chọn Telnet Client → OK

3.Tạo các OU và di chuyển các Computer Account vào trong OU tương ứng (thực hiện trên máy DC)

B1: Start → Programs →Administrative Tools → Active Directory Users and Computers

B2: Cửa sổ Active Directory Users and Computers → Click phải nhatnghe.edu → New → Organizational Unit (tạo 2 OU)

B3: Hộp thoại New Object → Nhập MyMemberServer → OK→Thao tác tương tự → Nhập MyClientComputers → OK→

4.Tạo các Group Policy Object_GPO (thực hiện trên MBRSRV)

B1: Start →Programs → Administrative Tools → Group Policy Management→Group Policy Management → Click phải Group Policy Objects →New

B2: hộp thoại New GPO → Nhập Firewall Settings for WS2008 Servers → OK→Firewall Settings for Vista Clients → OK

5.Bật Firewall trên các máy CLIENT (thực hiện trên MBRSRV)

B1:Cửa sổ Group Policy Management → Click phải Firewall Settings for Vista Clients → Edit

B2: Group Policy Management Editor → Click phải Firewall Settings for Vista Clients → Properties→Firewall Settings for Vista Clients … Properties → Chọn Disable User Configuration settings → Hộp thoại Confirm Disable → Yes → OK

B3: Group Policy Management Editor → Chọn Windows Firewall Properties→Windows Firewall with Advanced Security … → Tab Domain Profile → Firewall state chọn On (recommended) →OK

B4: Quan sát kết quả →Windows Firewall is on trong Domain Profile

6.Link GPO với OU (thực hiện trên MBRSRV)

B1:Cửa sổ Group Policy Management →Click phải MyClientComputers → Link an Existing GPO…

B2: Hộp thoại Select GPO → Chọn Firewall Settings for Vista Clients → OK

B3: Command line → gpresult /scope computer → Quan sát kết quả

B4: Windows Firewall with Advanced Security → Click phải Firewall with Advanced Security on Local Computer → Properties

B5: Windows Firewall … Properties → Tab Domain Profile → Firewall state: On (recommended) → OK

7.Local administrator tạo firewall rule→ xung đột với GPO đã được áp trên CLIENT (thực hiện trên CLIENT, log on bằng quyền Local administrator)

B1:Mở Command line → ping pc17.nhatnghe.edu (máy DC)→ Windows Firewall with Advanced Security →Click phải Outbound Rules → New Rule

B2: Rule Type → Chọn Custom → Next→Program → Chọn All programs → Next

B3: Protocol and Ports → Để mặc định → Next→Scope → Để mặc định → Next

B4: Action → Để mặc định → Next→Profile → Bỏ chọn Private và Public → Next

B5: Name → Nhập A Test Rule → Finish→Command line → ping pc17.nhatnghe.edu (máy DC)

B6: Windows Firewall with Advanced Security >→Click phải A Test Rule → Disable Rule

8.Ngăn cản các Firewall rule được tạo bởi Local administrators (thực hiện trên MBRSRV)

B1:Cửa sổ Group Policy Management → Click phải Firewall Settings for Vista Clients → Edit

B2: Group Policy Management Editor → Click phải Windows Firewall with Advanced Security … → Properties

B3: Windows Firewall with Advanced Security … Properties → Tab Domain Profile → Chọn Customize

B4: Customize Settings for Domain Profile → Firewall settings → Display a notification → Chọn No

B5: Customize Settings for Domain Profile → Rule merging → Apply local firewall rules → Chọn No

B6: Apply local connection security rules → Chọn No

Bài tập 2::Tạo Group Policy Object trên win2k2012

Yêu cầu: Tạo OU để quản lý và ủy nhiệm cho việc quản lý chức năng của OU là giúp triển khai chính sách (policy) ở cấp độ domain

Chuẩn bị

- Máy DC: 2012may1 IP: 192.168.2.100/24
- 1 máy computer member domain: 2012may2 192.168.2.101/21
- Tạo cấu trúc OU theo hình cây: OU CongTy chứa 2 OU con là KeToan, NhanSu
- Trong OU KeToan chứa: Group KT và KT1, Kt2. OU NhanSu làm tương tự

Hướng dẫn làm bài

B1: Run → gpmc.msc: Group Policy Management→ Control Panel => Tạo GPO ở OU công ty

B2: Chọn vào OU CongTy → Create a GPO in this domain and Link it here→ Khai báo tên GPO -> OK

B3: phải chuột GPO → Edit để tìm policy cấm control panel→ Enable Policy

B4: Cấm sử dụng IE→ User configuration →Policies → Administrative template → Windwos Component → Microsoft Management Console → Restricted/ Permitted Snap-in → Active Directories Sites and Services→Enbale Policy

B5: chọn vào OU KetToan → chọn Link an existing GPO →Cam mo→OK

BÀI 6:GIỚI THIỆU VỀ ISA SERVER
Mã bài:MĐ 24-06

Thời gian: 4 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày được tầm quan trọng của ISA Server trong việc bảo vệ hệ thống mạng;
- Xác định được các tính năng trên ISA Server
- Trình bày khái quát các khả năng và nét đặc trưng của ISA Server
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1. Định nghĩa Firewall

Firewall là một kỹ thuật được tích hợp vào hệ thống mạng chống lại việc truy cập bất hợp pháp của các hacker nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin không mong muốn. Firewall là một giải pháp dựa trên phần cứng và phần mềm dùng để kiểm tra dữ liệu đi từ bên ngoài vào máy tính hoặc từ máy tính ra ngoài mạng Internet.

2. Phân loại Firewall

2.1. Firewall phần mền

- Tính linh hoạt cao: có thể thêm bớt các quy tắc, các chức năng.
- Firewall mềm hoạt động ở tầng cao hơn Firewall cứng (tầng ứng dụng).
- Firewall mềm có thể kiểm tra nội dung gói tin thông qua các từ khóa

2.2. Firewall phần cứng

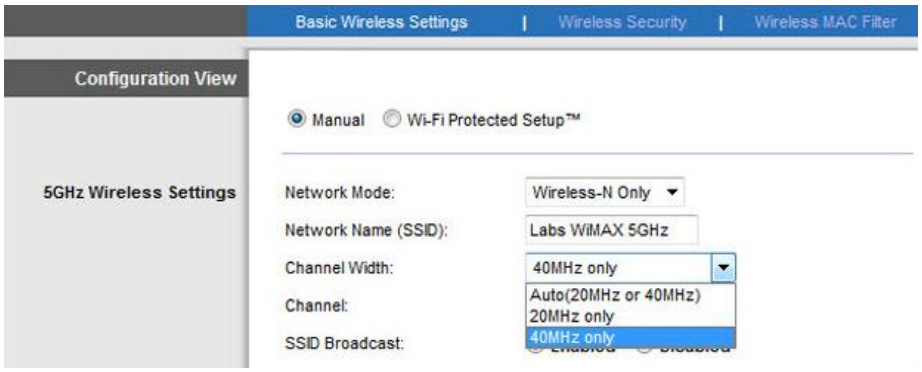
- Không được linh hoạt như Firewall mềm (không thể thêm chức năng thêm quy tắc như Firewall mềm).
- Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm (tầng Network và tầng Transport)
- Firewall cứng không thể kiểm tra được nội dung gói tin.

2.3. Bộ định tuyến không dây

Các router đời mới đều có sẵn hệ thống tường lửa riêng để bảo vệ người dùng khỏi các hiểm họa từ Internet.

Độ rộng băng tần (Channel Width)

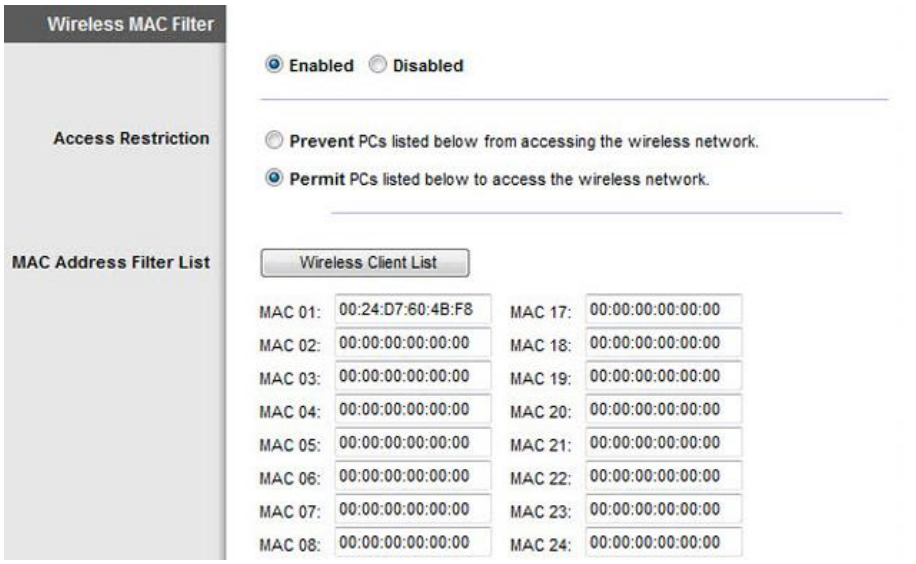
Thay đổi độ rộng băng tần là thay đổi số lượng băng tần có thể sử dụng cho việc truyền dữ liệu. Độ rộng băng tần có thể được thay đổi cho cả dải 2,4 và 5GHz, với các tùy chọn 20MHz, 40MHz và thậm chí lên tới 60MHz trên các router hỗ trợ chuẩn 802.11ac mới nhất.



Hình 6-1:Cửa sổ độ rộng băng tần

Bộ lọc địa chỉ MAC (MAC Filtering)

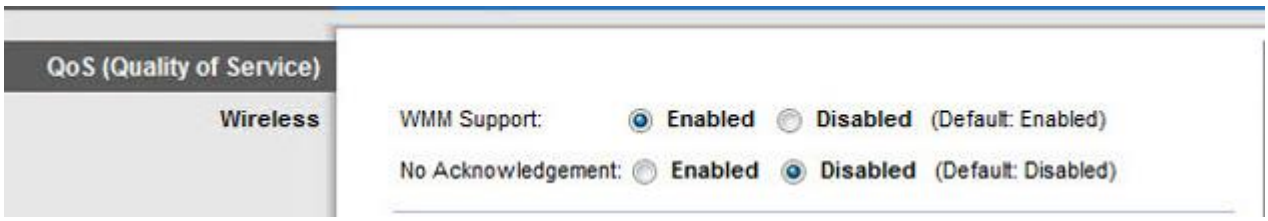
Địa chỉ MAC – địa chỉ độc nhất của mỗi card mạng là một trong những công cụ tốt nhất để quản lí kết nối. Để tăng cường bảo mật cho hệ thống mạng không dây của bạn, việc đầu tiên cần nghĩ đến là chọn cấu hình phù hợp cho bộ lọc địa chỉ MAC



Hình 6-2: Cửa sổ bộ lọc địa chỉ MAC

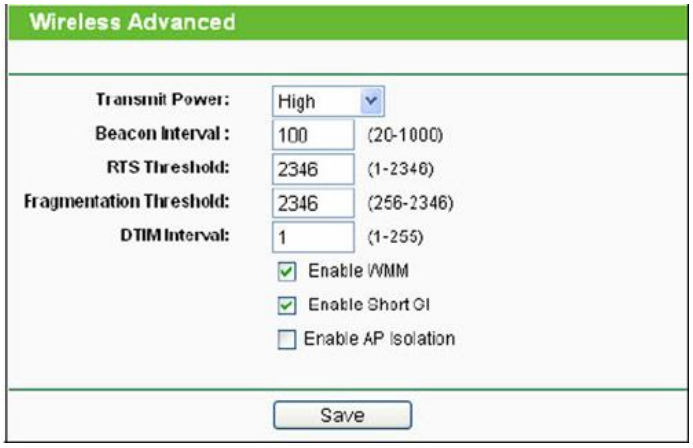
Quality of Service (QoS) là chức năng giúp tăng chất lượng kết nối cho một số nhu cầu hoặc ứng dụng cụ thể như các ứng dụng stream video, game, VoIP. Phần lớn các router có sẵn một dạng QoS nào đó, một số nhà sản xuất còn thiết bị mạng còn bán riêng các phiên bản router được cài đặt QoS cao cấp

Hỗ trợ Wifi Multimedia (WMM) là một dạng QoS tự động được tích hợp sẵn trong hầu hết các router để đảm bảo các ứng dụng đa phương tiện truyền tải hình ảnh và âm thanh một cách hiệu quả nhất


QoS (Quality of Service)
Wireless
WMM Support: Enabled Disabled (Default: Enabled)
No Acknowledgement: Enabled Disabled (Default: Disabled)

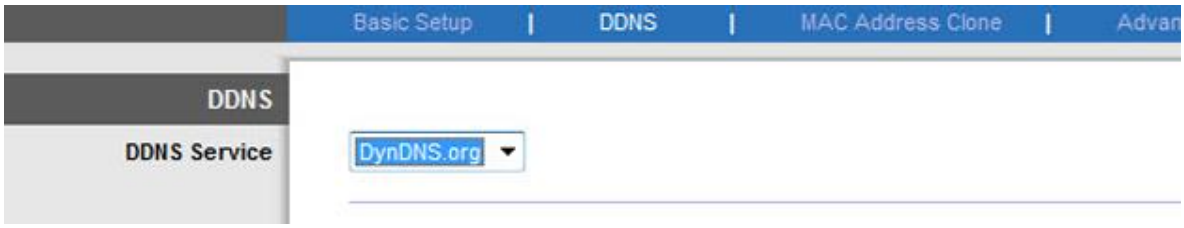
Hình 6-3:Cửa sổ Hỗ trợ Wifi Multimedia

Các cấu hình nâng cao



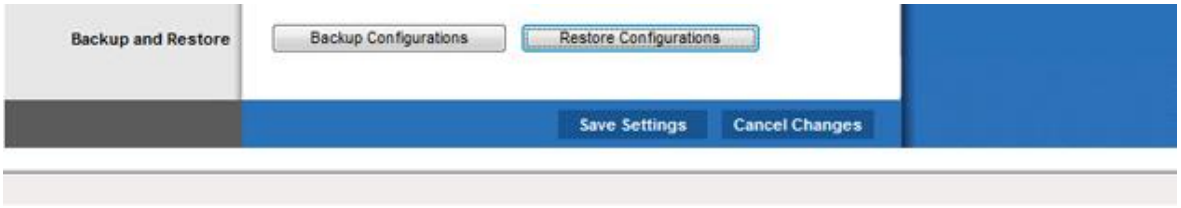
Hình 6-4:Cửa sổ cấu hình nâng cao

DNS động Dynamic DNS (DDNS) Khi sử dụng DDNS, người dùng có thể gán IP public động của router nói riêng và mạng nhà mình nói chung cho một tên miền.



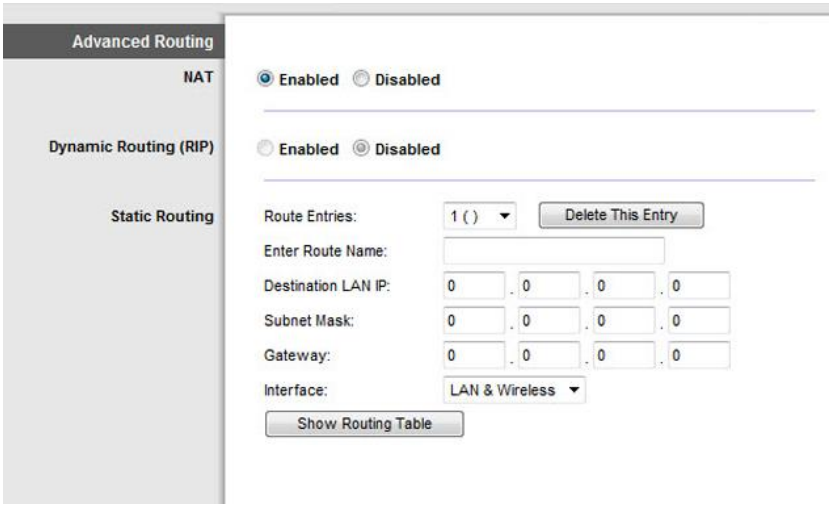
Hình 6-5: Cửa sổ DNS động

Sao lưu và khôi phục (Backup and Restore)



Hình 6-6: Cửa sổ sao lưu và khôi phục

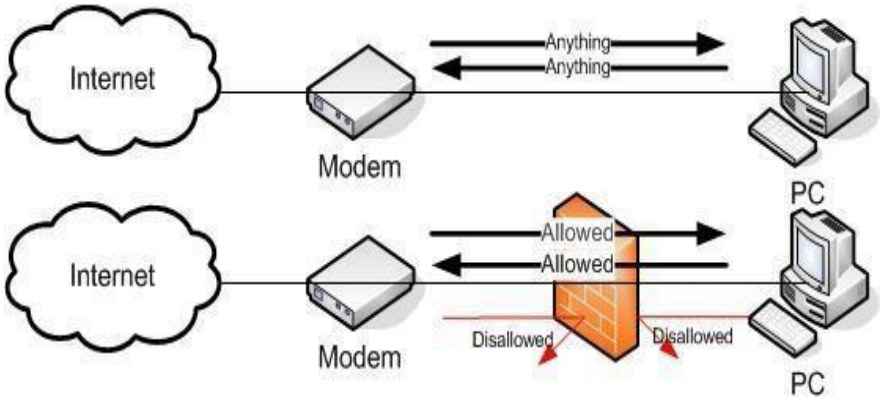
Network Address Translation (NAT) hường được sử dụng để chuyển thông tin nguồn gửi tin từ địa chỉ IP LAN trong mạng nhà hoặc công ty bạn thành địa chỉ IP Public ISP cấp cho bạn trước khi gửi đi.



Hình 6-7: Cửa sổ Network Address Translation

3. Chức năng của Firewall

Kiểm soát dịch vụ



Hình 6-8:Kiểm soát nguồn thông tin giữa mạng Internet và máy tính

- Cho phép /không cho phép những dịch vụ truy cập từ hệ thống ra bên ngoài.
- Cho phép/ không cho phép những dịch vụ truy cập từ ngoài vào trong hệ thống
- Kiểm soát địa chỉ truy cập của người dùng và nội dung nhận được từ Internet
- Chống lại những đợt tấn công bất hợp pháp của Hacker

4. Các kiến trúc Firewall cơ bản

4.1. Tường lửa bộ lọc gói tin (Packet filtering firewall)

Loại Firewall này thực hiện việc kiểm tra số nhận dạng địa chỉ của các Packet để cho phép chúng có thể lưu thông qua lại hay không, các thông số có thể lọc được một Packet như sau:

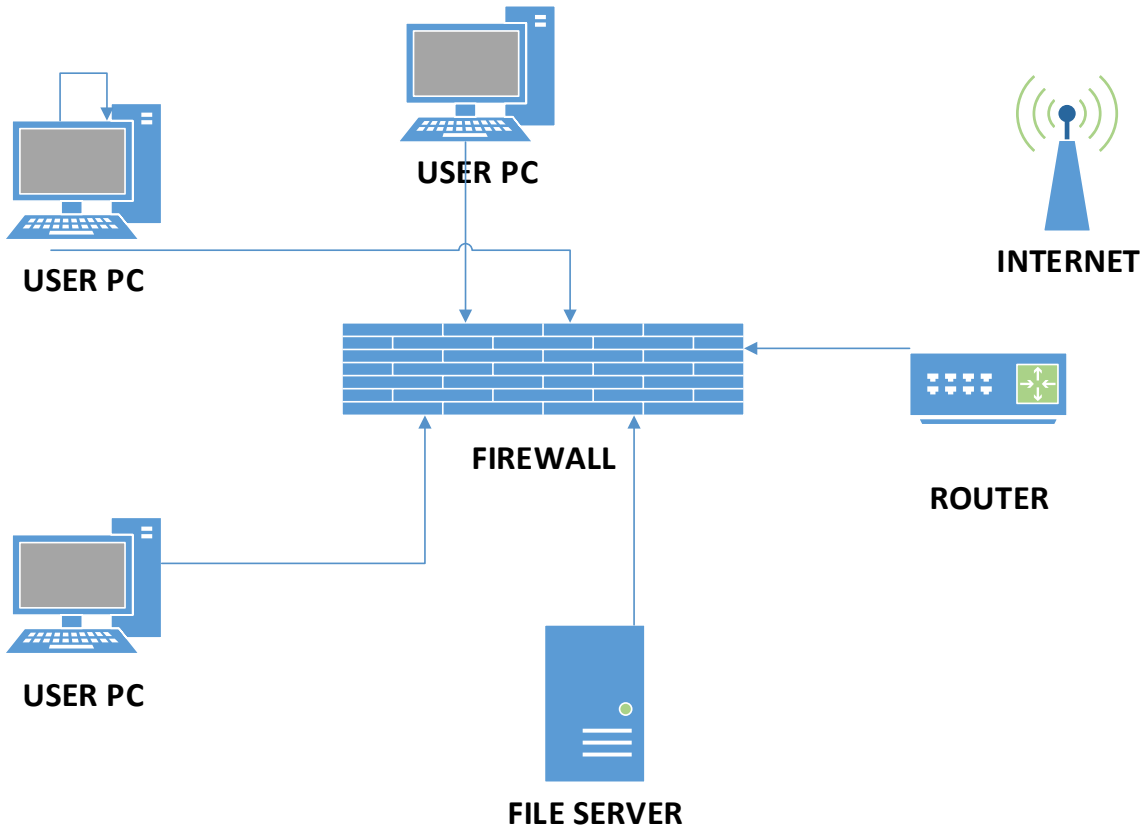
Địa chỉ IP nơi xuất phát (source IP address).

Địa chỉ IP nơi nhận (destination IP address).

Cổng TCP nơi xuất phát (TCP source port).

Cổng TCPnơi nhận (TCP destination port).

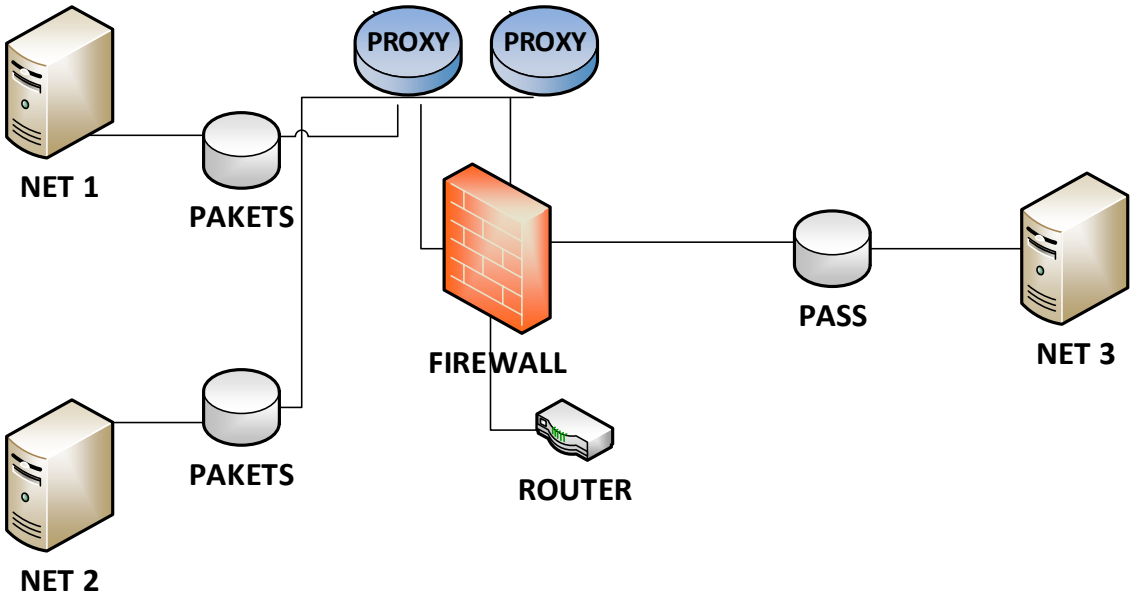
Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào những máy chủ hoặc khóa viêc truy cập vào hệ thống nội bộ từ những địa chỉ không cho phép.



Hình 6-9: Sơ đồ tường lửa bộ lọc gói tin

4.2. Cổng tần ứng dụng (Application gateway)

Cổng tầng ứng dụng là một thiết bị bảo mật dùng để phân tích các gói dữ liệu được chuyển vào. Khi các gói dữ liệu từ bên ngoài đến cổng, chúng được kiểm tra và xác định xem chính sách bảo mật có cho phép chúng vào mạng hay không. Máy phục vụ không chỉ định giá trị các địa chỉ IP mà còn xem xét dữ liệu trong các gói để tìm lỗi và sửa sai.



Hình 6-10:Sơ đồ tường lửa cổng tầng ứng dụng

Một cổng tầng ứngdụng điển hình có thể cung cấp các dịch vụ ủy quyền cho các ứng dụng và giao thức như Telnet, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), SMTP(Simple Mail Transfer Protocol), và cổng ứng dụng này không cho phép bất kỳ gói tin nào đi thẳng trực tiếpgiữa hai mạng.

Khi trạm bên ngoài muốn kết nối với các trạm bên trong tường lửa thông qua một dịch vụ nào đó thì trạm bên ngoài phải thông qua Proxy Service. Nếu dịch vụ và địa chỉ trạm bên ngoài không thuộc diện cấm thì Proxy Service sẽ đi tìm trạm đích bên trong tường lửa để tạo kết nối với trạm bên ngoài và ngược lại các trạm bện trong kết nối ra ngoài cũng vậy. Với cách thức này sẽ đánh bại được một số loại tấn công gây tràn bộ đệm của tường lửa.

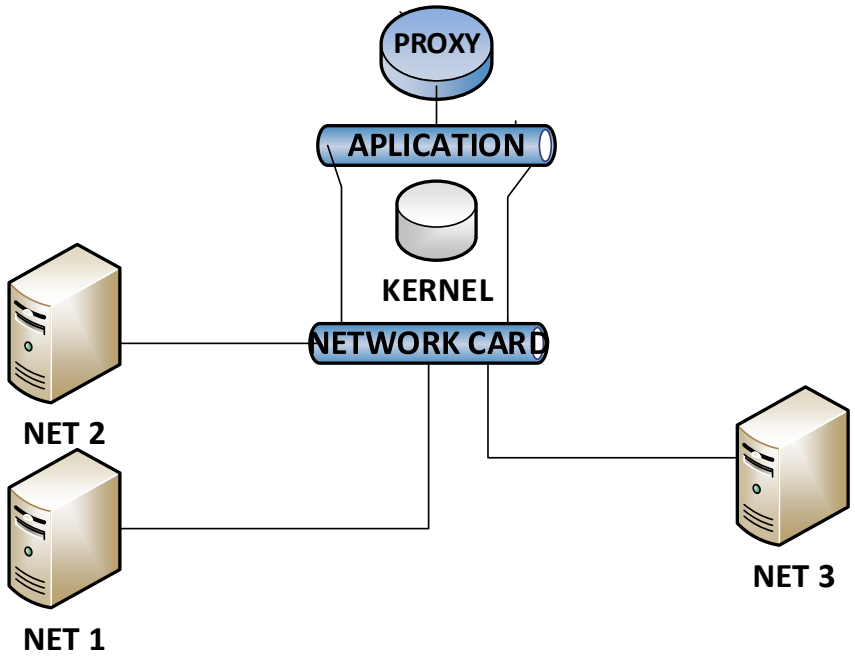
4.3. Bastion Host Firewall (Pháo đài phòng ngự).

Một trạm được cấu hình để chặn đứng mọi cuộc tấn công từ phía bên ngoài vào. Đây là điểm giao tiếp trực tiếp với mạng không tin cậy bên ngoài do đó dễ bị tấn công nhất. Có hai dạng máy phòng thủ.

5. Giới thiệu về ISA server

5.1.Điều Khiển Truy Nhập (Access Control)

Có 3 đường dẫn phổ biến mà một gói tin có thể đi qua tùy thuộc vào dạng tường lửa cài đặt. Một gói tin có thể vượt qua tường lửa ở mức tầng ứng dụng, ở mức nhân hệ điều hành hoặc là mức card giao tiếp mạng. Hầu hết các tường lửa đều kiểm soát và cho phép các gói tin đi qua 3 mức này



Hình 6-11: Sơ đồ điều khiển truy nhập

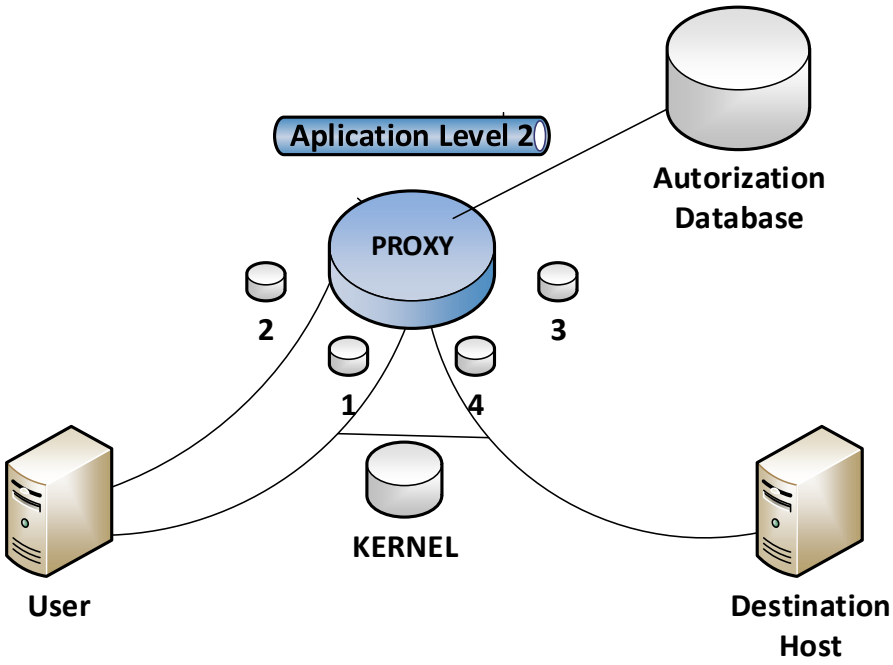
Luật lọc (Filtering Rules): Bộ lọc sẽ kiểm tra 5 mảng thông tin trong khối IP ở phần đầu của gói tin các thông tin đó bao gồm:

Source IP address	Địa chỉ IP của trạm nguồn gởi gói tin.
Destination IP address	Địa chỉ IP của trạm đích gói tin sẽ đi tới.
Upper level Protocol (đó là TCP hoặc	Cho giao thức khác và dịch vụ khác
TCP or UDP source port number	Số hiệu cổng của trạm nguồn gởi gói ra.
TCP or UDP destination port number	Số hiệu cổng của trạm đích sẽ nhận gói tin.

5.2.Vị trí xảy ra quá trình xử lý gói

Khi có được thông tin trên của các gói, bộ lọc sẽ so sánh chúng với một tập hợp các luật để đưa ra quyết định. Một luật lọc là sự kết hợp một giá trị hoặc miền giá trị của mỗi trường thông tin trên và quyết định sẽ đưa ra nếu tất cả các thông tin của gói được so khớp với các thông tin các luật.

Hoạt động của tường lửa người đại diện ứng dụng (Proxy Application):



Hình 6-12: Sơ đồ quá trình xử lý gói

5.3.Luật lọc (Filtering Rules).

Người sử dụng sẽ chạy ứng dụng đặt biệt để tạo kết nối đến tường lửa. Người sử dụng chỉ việc cung cấp tên hoặc địa chỉ trạm đích cho ứng dụng hỗ trợ. Địa chỉ tường lửa sẽ được ứng dụng hỗ trợ này lấy ra từ file cấu hình cục bộ sau đó sẽ thiết lập kết nối đến người đại diện trên tường lửa. Giải pháp này tỏ ra hữu hiệu và trong suốt đối với người sử dụng tuy nhiên hạn chế của nó là mỗi chương trình hỗ trợ máy khách chỉ thực hiện tương ứng với một dịch vụ nào đó của mạng mà thôi.

5.4 Hoạt động của tường lửa người đại diện ứng dụng (Proxy Application)

Một phương pháp nữ được sử dụng hiện nay cho việc kết nối đến đại diện ứng dụng trên tường lửa là sử dụng đại diên tàng hình(ẩn). Với giải pháp này thì người sử dụng không cần đến chương trình hỗ trợ máy khách hoặc kết nối trực tiếp đến tường lửa.

5.5.Quản lý xác thực (User Authentication)

Đây là chức năng ngăn cản việc truy cập trái phép vào hệ thống mạng nội bộ. Các hệ điều hành quản lý mạng chỉ kiểm soát một cách không chặt chẽ tên người sử dụng và password được đăng ký.

Có hai giao thức chuẩn thông dụng nhất hiện nay để kết hợp làm việc với LAN.

RADIUS (Remote Authen-tication Dial-In User Service).

TACASE (Terminal Access Controller Access Control System Extended).

5.6.Kiểm tra và Cảnh báo (Activity Logging and Alarms)

5.6.1.Activity logging

Các thông tin này rất hữu ít cho việc phát hiện kịp thời những lỗ hổng trên tường lửa. Một log files chuẩn phải có những thông tin sau:

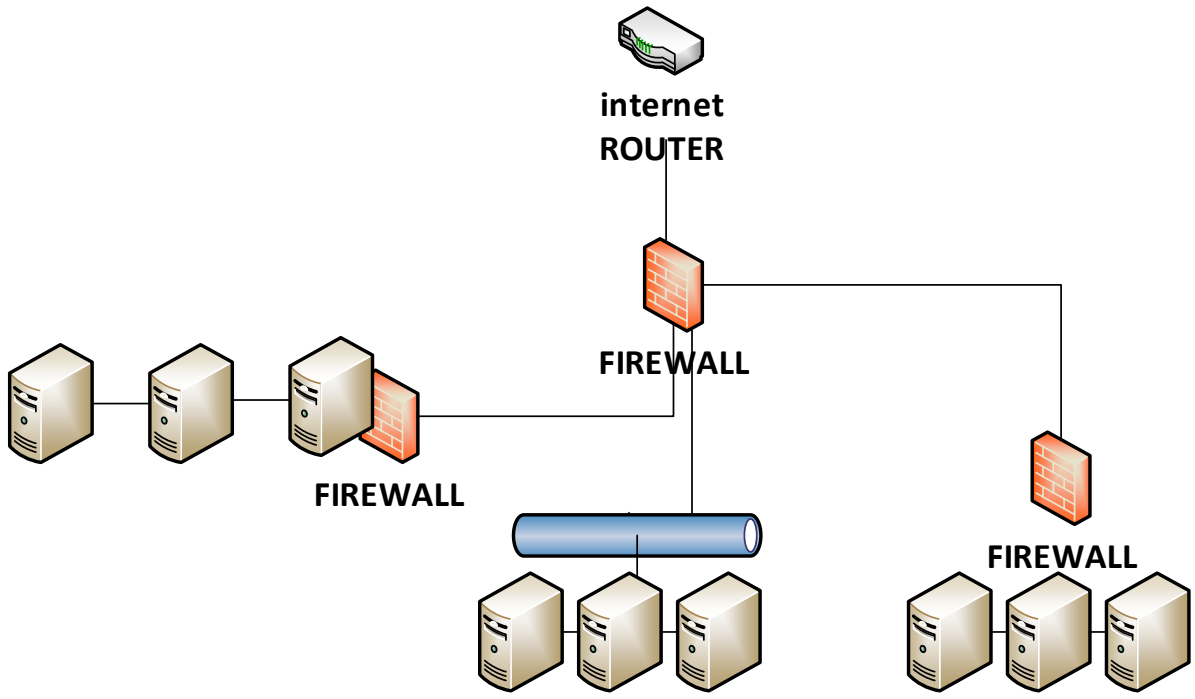
+ Thời gian bắt đầu và kết thúc của một phiên. Địa chỉ trạm nguồn.
+ Địa chỉ trạm đích.
+ Giao thức sử dụng (TCP hay UDP). Cổng được mở trên trạm đích.
+ Kết quả của việc kết nối(thành công hay bị từ chối).
+ Tên người sử dụng nếu xác thực được sử dụng.

5.6.2.Alarm

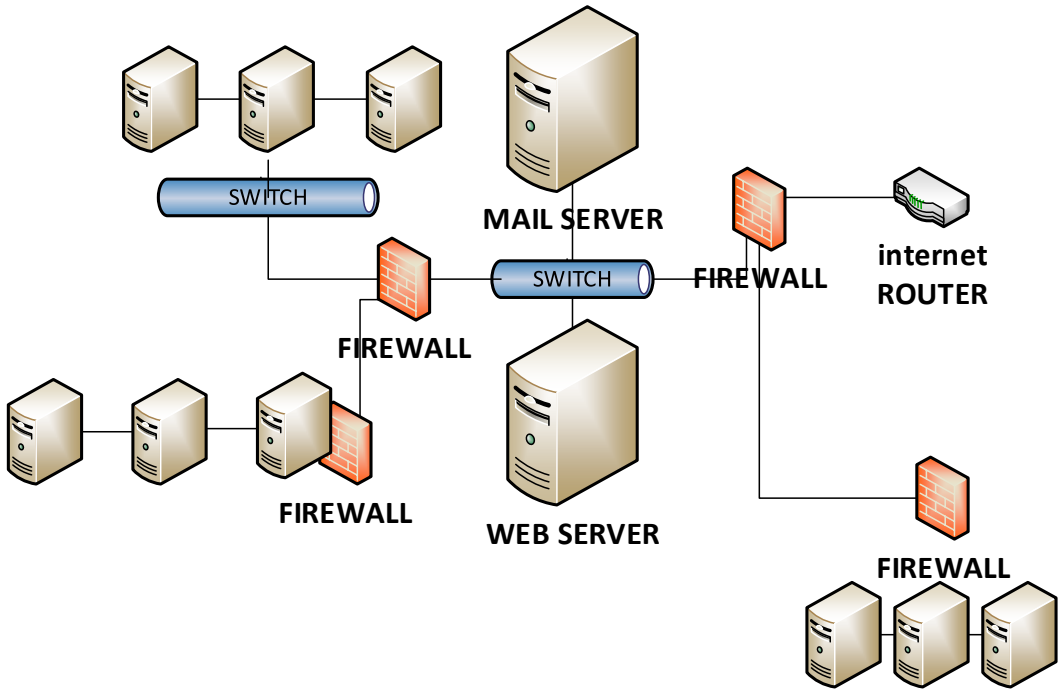
Khi một gói bị chặn lại không qua được tường lửa thì hoạt động cảnh báo của tường lửa cũng gởi một cảnh báo đến trạm nguồn thông báo về nguyên nhân loại bỏ gói đó.

5.7.Các mô hình Firewall cơ bản và phức tạp

Mô hình Firewall cơ bản thường sử dụng

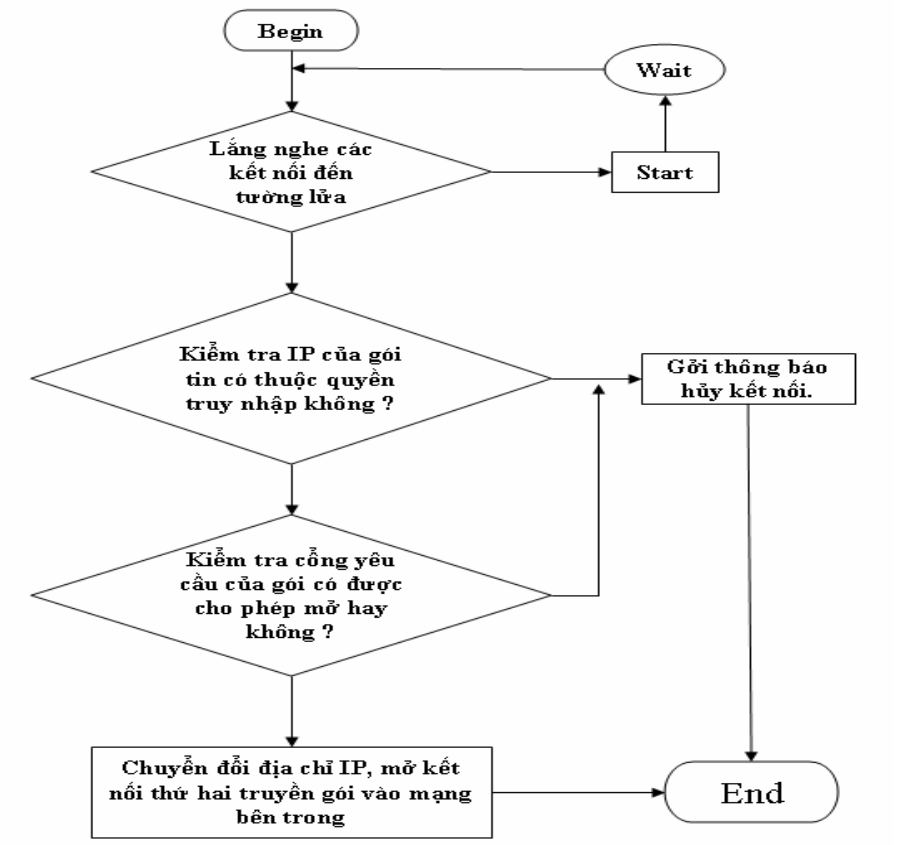


Hình 6-13:Mô hình Firewall sử dụng cho các doanh nghiệp lớn



Hình 6-14:Mô hình Firewall sử dụng cho các doanh nghiệp lớn

5.8.Sơ Đồ hoạt động của ISA


Begin
Wait
Lắng nghe các kết nối đến tường lửa
Start
Kiểm tra IP của gói tin có thuộc quyền truy nhập không ?
Gởi thông báo hủy kết nối.
Kiểm tra cổng yêu cầu của gói có được cho phép mở hay không ?
Chuyển đổi địa chỉ IP, mở kết nối thứ hai truyền gói vào mạng bên trong
End

Hình 6-15: Sơ Đồ hoạt động của ISA

6.TÓM TẮT NỘI DUNG

- Kiểm soát dữ liệu ra vào hệ thống mạng
- Kiểm soát quá trình truy cập của người dùng theo giao thức, thời gian và nội dung nhằm ngăn chặn việc kết nối vào trang web có nội dung không phù hợp.
- Cho phép triển khai các mạng riêng ảo tích hợp để bảo mật
- Ứng dụng cho các mô hình mạng doanh nghiệp

7- CÂU HỎI

Câu 1: Trình bày về firewall:Khái niệm, tại sao cần có firewall. Các kỹ thuật điều khiển truy cập trong firewall, hạn chế của firewall. Các loại firewall:packet-filtering firewall, application -level gateway, circuit-level gateway. Cơ chế hoạt động của từng loại.

Câu 2: Trình bày về packet-filtering firewall:Khái niệm, cơ chế, ưu nhược điểm của packet-filtering firewall. Các biện pháp thường được sử dụng để tấn công packet-filtering firewall: IP Spoofing, Source routing attack, Tiny fragment attack. Stateless và Stateful firewall. Ưu điểm của Stateful firewall so với Stateless firewall.

Câu 3: Trình bày đặc điểm của ISA 2006.

Câu 4: Vẽ sơ đồ hệ thống mạng sử dụng Firewall

BÀI 7: CÀI ĐẶT VÀ CẤU HÌNH SỬ DỤNG CÁC RULE TRONG ISA
Mã bài:MĐ 24-07

Thời gian: 13 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Cài đặt được ISA Server trên windows Server theo đúng qui trình;
- Thiết lập được các rule để bảo mật cho hệ thống.
- Thực hiện các thao tác an toàn với máy tính.

II.NỘI DUNG CHÍNH

Mục tiêu: *Cài đặt được ISA Server trên windows Server theo đúng qui trình*

1.Cài đặt ISA

1.1 Chuẩn bị: Cài đặt ISA 2006 bản standart

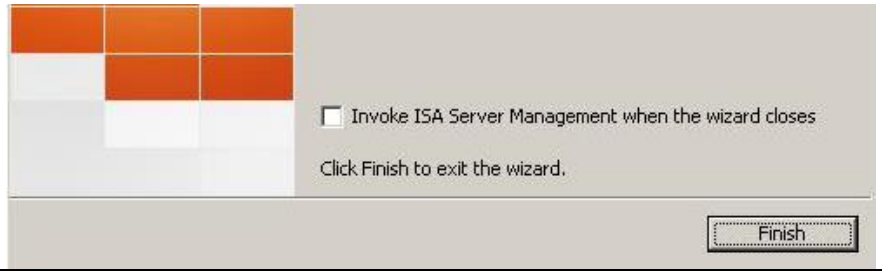
- Trên máy isa nên disable card internet, rồi sau đó gia nhập domain.
- Để cài đặt được ISA thì sau khi máy isa khởi động lại phải sử dụng user name và password của máy domain mới có thể cài được, sau đó enable card internet lên.

1.2 Thực hiện

Bước 1: Hộp thoại → Next→Next→ I accept → Next→Next→ Typical → Next

Microsoft ISA Server 2006 - Installation Wizard
Setup Type
Choose the setup type that best suits your needs.
Typical
Main program features will be installed.

Bước 2: Internal Network → Add→ Add adapter → check chọn Card LAN → OK→Next→Next→Next→ Install…. → finish



Bước 3: Cài bản vá sp1→Next→ I accept → Next→ Install→ Finish

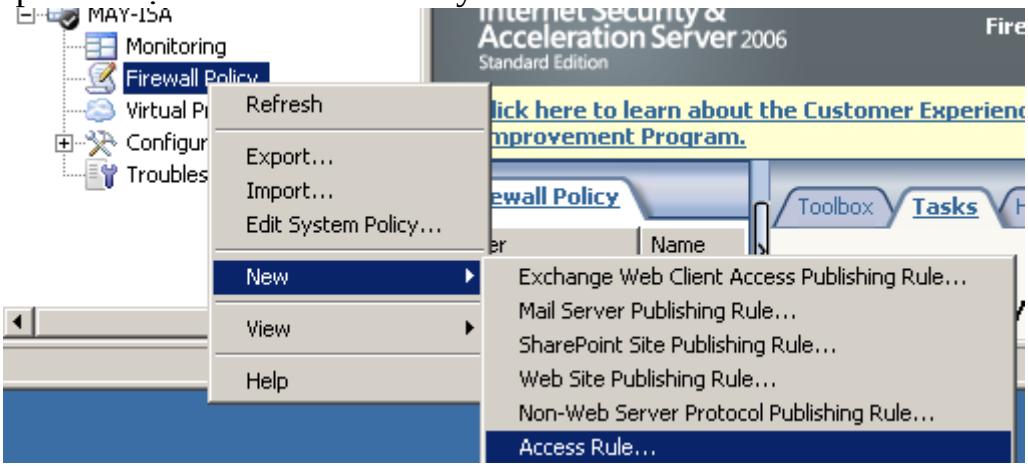
Hệ thống yêu cầu khởi động lại máy → Yes

2.Tạo rule cho Admin đi ra ngoài Internet sử dụng tất cả các giao thức

Cài đặt

Bước 1: Cài đặt Rule

Click phải chuột vào Firewall Policy → New → Access Rule



Đặt tên "TRUYCAP-INTERNET" → Next

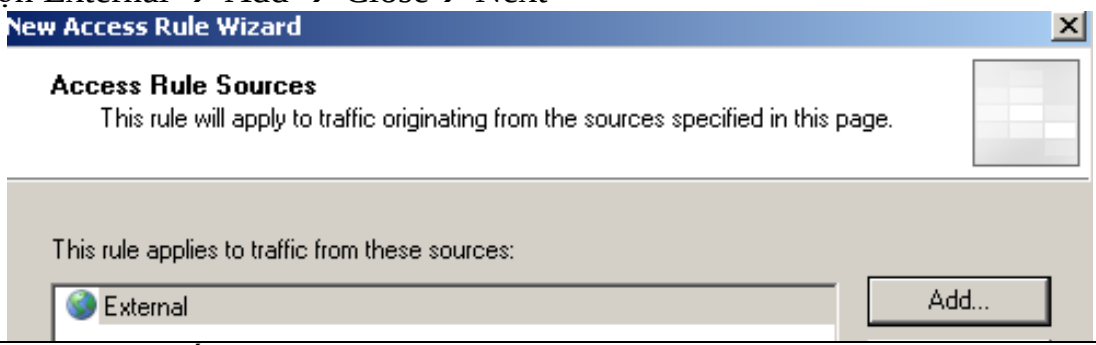
Chọn Allow cho phép → Next

Bước 2: Cấu hình Rule

Hộp thoại New Access Rule→ Selected protocols →HTTP, HTTPS→Add →Close→next

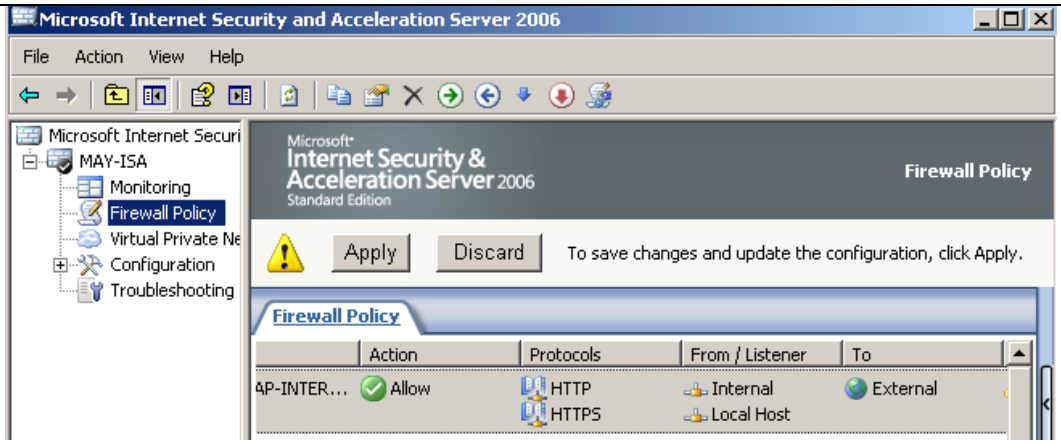
Chọn Internal, Local Host→ Add → Close→ Next

Chọn External → Add → Close→ Next


New Access Rule Wizard
Access Rule Sources
This rule will apply to traffic originating from the sources specified in this page.
This rule applies to traffic from these sources:
External
Add...

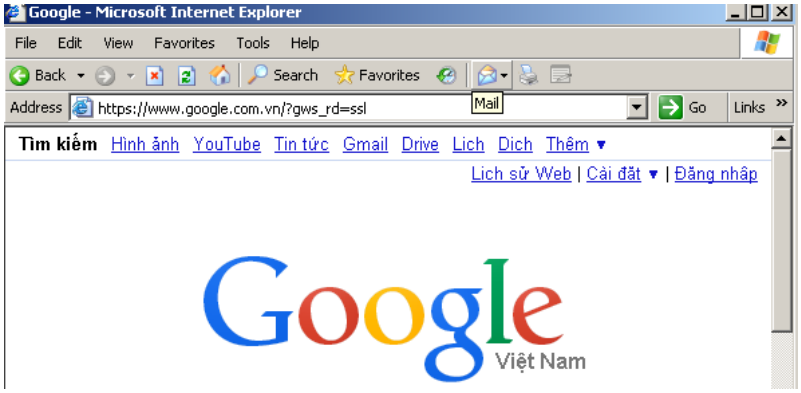
Bước 3: Hoàn tất tạo Rule

- Hộp thoại User Sets: Mặc định cho phép tất cả User → Next
- Chọn Finish để kết thúc tạo Rule.
- Chọn Apply



- Chọn OK. Để cập nhật

Bước 4: Kết nối intenet trên máy ISA và máy DC nhận thấy đã truy cập thành công



3.Cấu hình cho các clien ra Internet chỉ sử dụng giao thức HTTP, HTTPS

Cấu hình

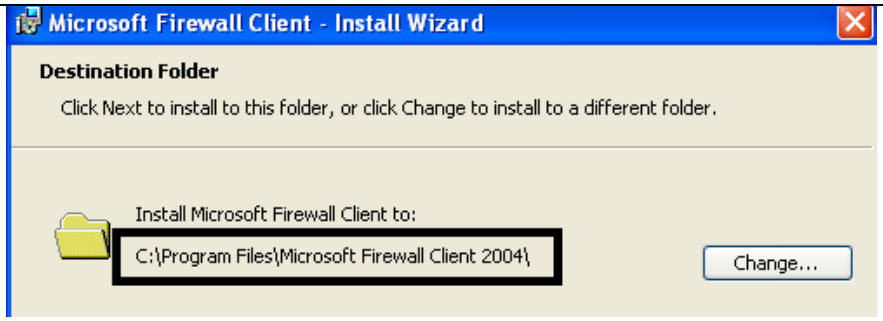
Bước 1: Khởi tạo cài đặt Firewall client

- Vào thư mục client chạy file setup firewall client→Run

- Hộp thoại Welcome to.. → Next
- Hộp thoại Lincense Agreement chọn I accept … → Next

Bước 2: Cài đặt Firewall client

- Chọn đường dẫn cài đặt → Next


Microsoft Firewall Client - Install Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Microsoft Firewall Client to:
C:\Program Files\Microsoft Firewall Client 2004\
Change...

- Hộp thoại ISA Server Computer
- Selection: chọn chế độ tự động→ Next
- Chọn Install để bắt đầu cài đặt

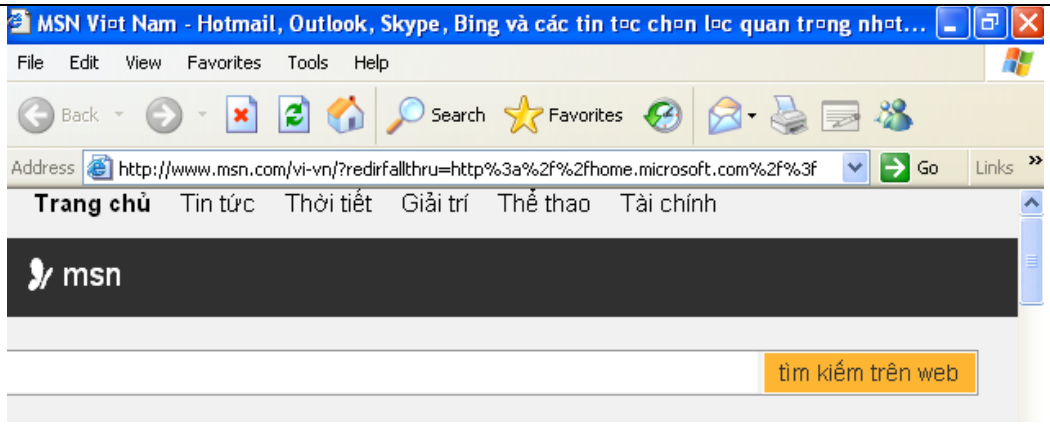
Bước 3: Hoàn tất cài đặt

- Hộp thoại Firewall client thông báo đã hoàn tất quá trình kết nối→OK

Bước 5: Cập nhật

- Hộp thoại Firewall client→Apply Default Settings Now để cập nhập→OK
- Biểu tượng Firewall client trên thanh taskbar thông báo đã mở kết nối

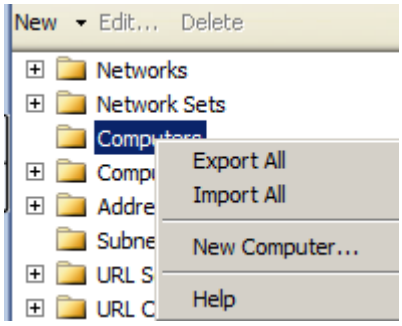
Kết nối internet trên máy XP nhận đã thấy truy cập thành công


MSN Vi¤t Nam - Hotmail, Outlook, Skype, Bing và các tin t¤c ch¤n l¤c quan tr¤ng nh¤t...
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.msn.com/vi-vn/?redirfallthru=http%3a%2f%2fhome.microsoft.com%2f%3f
Go Links
Trang chủ Tin tức Thời tiết Giải trí Thể thao Tài chính
msn
tìm kiếm trên web

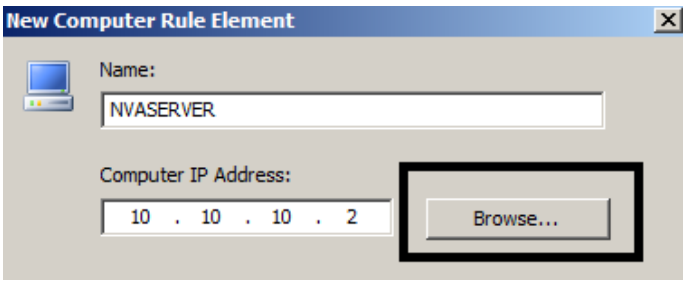
4.Cấu hình DNS phân giải tên

Cấu hình

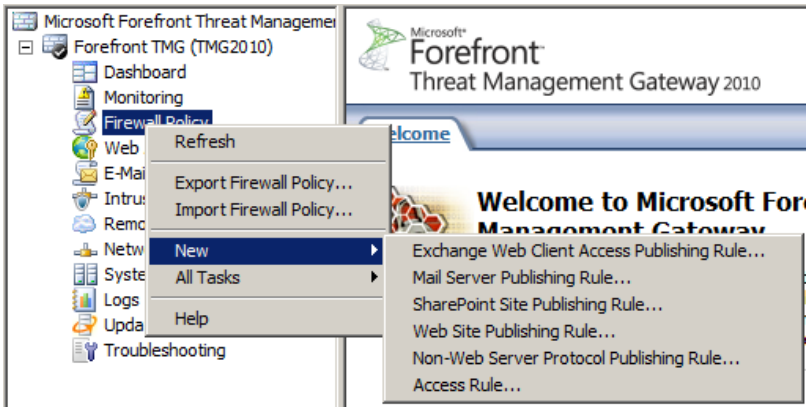
Bước 1: Chọn phần **Toolbox (TMG)** → Click – Phải **Computer** → **New Computer…**



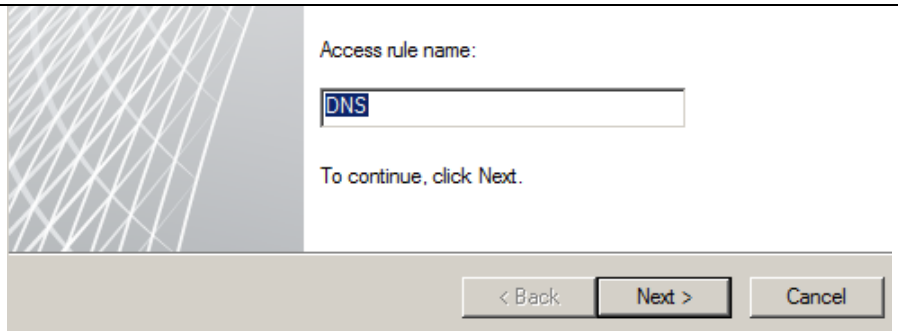
Bước 2: Ở đây ta tìm đến tên domain server **Browse…** → OK



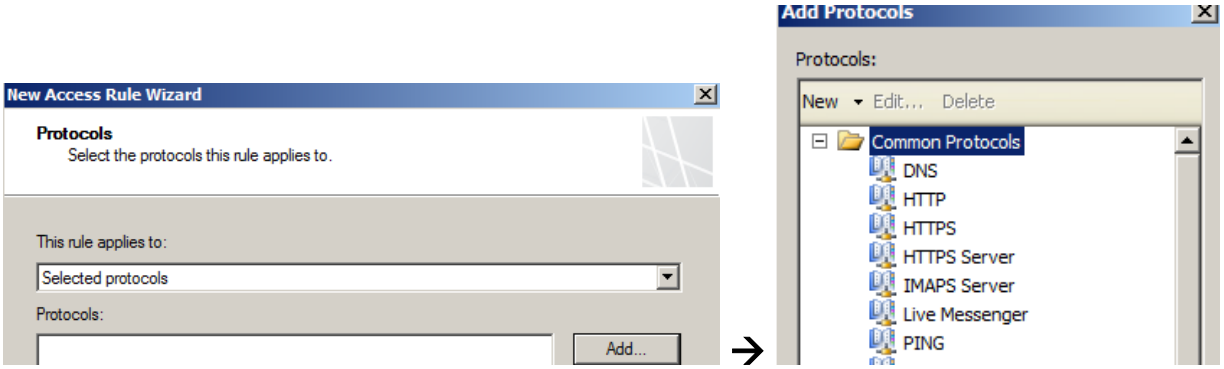
Bước 3: Click – Phải Firewall Policy → New → Access Rule…



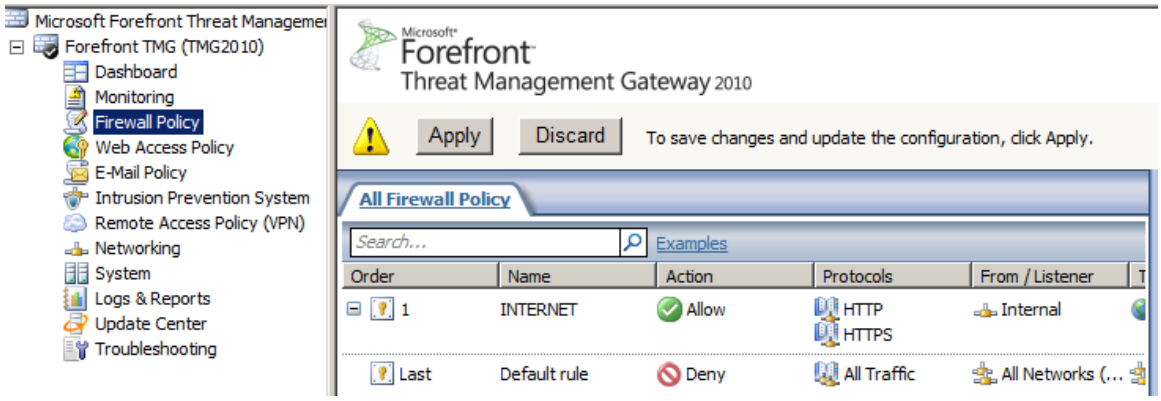
Bước 4: Tên Rule → Next



Bước 5: Chọn Add.. → Common Protocols → DNS → Close



Bước 6: Click → Apply → Apply



5.TÓM TẮT NỘI DUNG

- Cho phép người dùng và thông tin ứng dụng được ghi lại trong file bản ghi của tường lửa ISA
- Cung cấp hỗ trợ nâng cao cho các ứng dụng mạng gồm giao thức phức hợp có yêu cầu đến kết nối thứ cấp
- Cung cấp hỗ trợ "proxy" DNS cho tường lửa máy tính
  Cho phép bạn đưa ra các máy chủ yêu cầu giao thức phức hợp mà không cần sự hỗ trợ của bộ lọc ứng dụng
- Cơ sở hạ tầng định tuyến mạng là trong suốt đối với tường lửa máy khách
  Cho phép thẩm định dựa trên nhóm người dùng hoặc người dùng riêng biệt đối với các ứng dụng Winsock bằng sử dụng giao thức TCP và UDP

6.CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

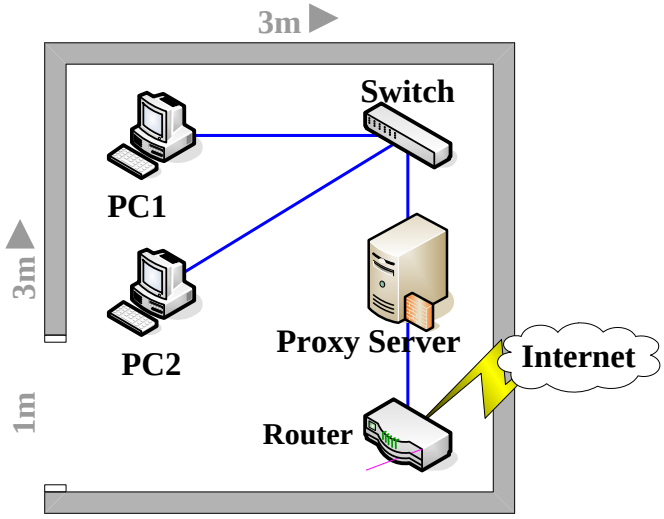
Câu 1: Trình bày Windows Firewall with Advanced Security trên Windows Server 2008

Câu 2: Trình bày firewall rule, Inbound Rules và Outbound Rules

Câu 3: Trình bày cách thức tạo một firewall rule

BÀI TẬP

Bài tập 1: Cho mô hình mạng



Yêu cầu:

1. Chọn các thiết bị mạng phù hợp để thiết lập mạng LAN cho cabin làm việc trên.
2. Chọn vị trí đặt Switch và các thiết bị kết nối sao cho tối ưu nhất (*tiết kiệm về dây cable và thiết bị khác).*
3. Lắp đặt mạng LAN theo sơ đồ trên.
4. Chọn 01 máy tính cài đặt Windows Sever 2003 trên PC1 và 02 máy tính còn lại cài đặt Windows XP. Cài đặt office 2003, Vietkey trên máy PC2
5. Cấu hình các máy tính trong mạng để chia sẻ file và truy cập Internet thông qua router.
6. cấu hình chỉ có user TUNG và TUAN được truy cập thư mục đang chia sẻ (share) trên máy Domain Controller
7. Cài đặt và cấu hình ISA 2006 cho PC 2 vào internet sau đó sao lưu cấu hình

Chuẩn bị:

- 1 máy PC cài win2k3→DC
- 2 máy PC cài win XP
- 1 switch
- Router internet
- Đấu nối theo mô hình
- Thiết lập địa chỉ IP cùng lớp mạng

Hướng dẫn làm bài

B1:Cài đặt office 2003, Vietkey trên máy PC2

B2: Tạo 2 User là : tung va tuan→ Chia sẻ thư mục cho 2 User→ Ở Client 1 gia nhập Domain với User tung

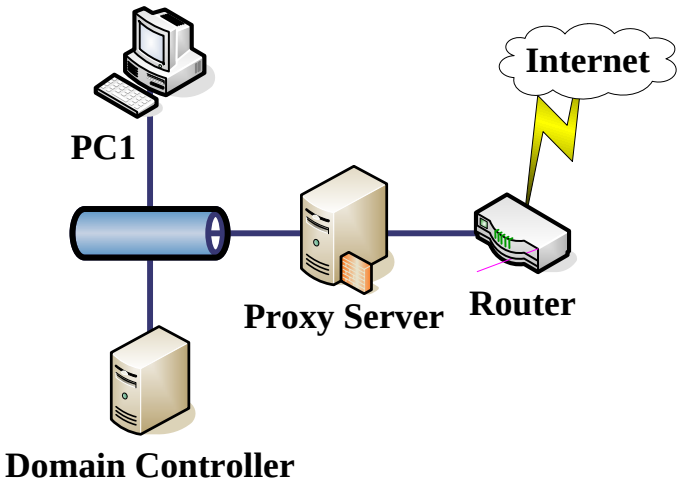
B2: Cài đặt ISA 2006→ Install ISA Server 2006→card kết nối ISA và Client →Next→Finish

B3: Start→ Program→Microsoft ISA Server→ISA Server Manager tạo Rule Acess để PING

B4: Tạo Rule "INTERNET" để cho phép các máy vô INTERNET

B5:Lưu cấu hình ISA

Bài tập 2: Cho mô hình mạng



<u>Yêu cầu:</u>

Mọi người khi truy cập Internet đều phải thông qua Proxy Server, và không được phép thay đổi địa chỉ Proxy.

Trên máy làm việc, mọi người khi đăng nhập vào hệ thống thì sẽ tự động ánh xạ thư mục dùng chung trong mạng về máy (Map Network Drive).

Trên Server tạo, phân quyền tài khoản người dùng và nhóm như sau:

1. Nhóm BanGiamDoc gồm: Hung, Trong

2. Nhóm NhanVien gồm: Diep, Tuan, Tung

3. Mỗi người dùng có toàn quyền trên thư mục dành riêng của mình.
4. Trưởng phòng của mỗi phòng ban sẽ đọc được dữ liệu của các thành viên khác trong phòng. Trưởng phòng là tài khoản đầu tiên trong danh sách của mỗi nhóm.
5. Thư mục Public là thư mục dùng chung, mọi người có thể ghi dữ liệu lên đó nhưng chỉ xóa được những dữ liệu do mình tạo ra.

Chuẩn bị:

- 1 máy PC cài win2k3→DC
- 1 máy PC cài win 2k3→Proxy
- 1 máy PC cài win Xp→ Client
- Router internet
- Đấu nối theo mô hình
- Thiết lập địa chỉ IP cùng lớp mạng
- Cài đ ặt ISA 2006

Hướng dẫn làm bài

B1: Cài đặt DNS→Vào control panel → add or remove → networking serverices → DNS → OK.

B2: cấu hình DNS→Vào program → adminstra tool → DNS → R_click vào forwand lookup zone→new zone→ Next → finish

B3:Tạo Phân giải tên miền thành địa chỉ IP và ngược lại

B4: Cài đặt IIS→Vào control pannel → add or remove → application servies→Finish

B6: tạo 1 trang web mới →Vào start → program → administra tool → IIS→ Đặt tên cho web →lưu →Next→Next

B7:Tạo User→ chia sẻ thư mục

B8:truy c ập m áy client v ào internet proxy→ tools→ intent option→ connetion→ Lan settings→OK

B9: Nhập địa chỉ card ISA → port 8080→OK→ protion kick R→ chọn auto discovery ở mục intenall→ chọn 8080→PK

BÀI 8:DỊCH VỤ VIRTUAL PRIVATE NETWORK
Mã bài:MĐ 24-08

Thời gian: 11 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

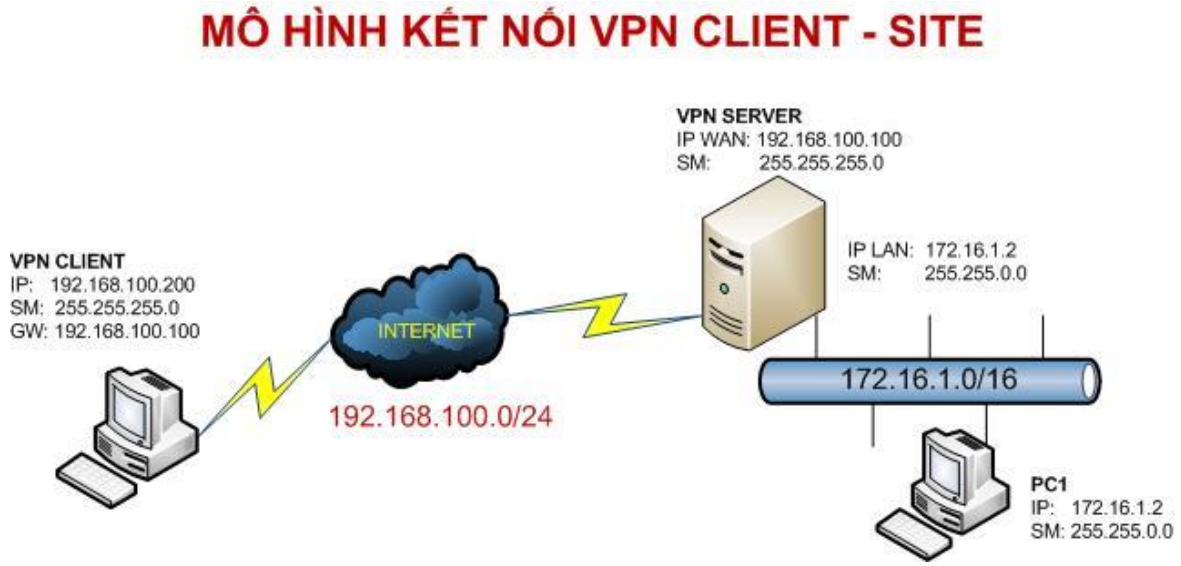
- Trình bày được bản chất và lợi ích của VPN
- Cài đặt, cấu hình được mô hình VPN to site;
- Cài đặt, cấu hình được mô hình site to site.
- Thực hiện các thao tác an toàn với máy tính.

II.NỘI DUNG CH ÍNH

1.Giới thiệu về VPN

1.1.Bản chất hoạt động của VPN

Về căn bản, mỗi VPN(virtual private network) là một mạng riêng rẽ sử dụng một mạng chung (thường là Internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa . Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường Leased Line, mỗi VPN sử dụng các kết nối ảo được dẫn qua đường Internet từ mạng riêng của công ty tới các site của các nhân viên từ xa.



Hình 8-1: mô hình VPN client to site

1.2.Lợi ích của VPN

Chi phí thấp: giảm thiểu việc lãng phí băng thông, khách hàng có thể trả theo cước lưu lượng sử dụng. Chúng ta hãy so sánh chi phí khi sử dụng đường thuê bao riêng và chi phí khi sử dụng Internet VPN .

Quản lý dễ dàng: trường có khả năng quản lý số lượng người sử dụng (khả năng thêm, xoá kênh kết nối liên tục, nhanh chóng). Hiện nay nhu cầu sử

dụng tư vấn từ bên ngoài, các nguồn lực từ bên ngoài để phục vụ cho công tác kinh doanh đã trở thành một xu hướng. - Khả năng lựa chọn tốc độ tối đa từ tốc độ 9,6 Kbit/s tới T1/E1, hoặc sử dụng công nghệ DSL.

Khả năng cung cấp dịch vụ một cách nhanh chóng: VPN được cung cấp trên mạng IP tích hợp được một số ưu điểm của mạng này đó là khả năng liên kết lớn, mạng lưới sẵn có vì vậy giảm thiểu thời gian cung cấp dịchvụ.

2.Mô hình VPN Client to Site dùng giao thức PPTP

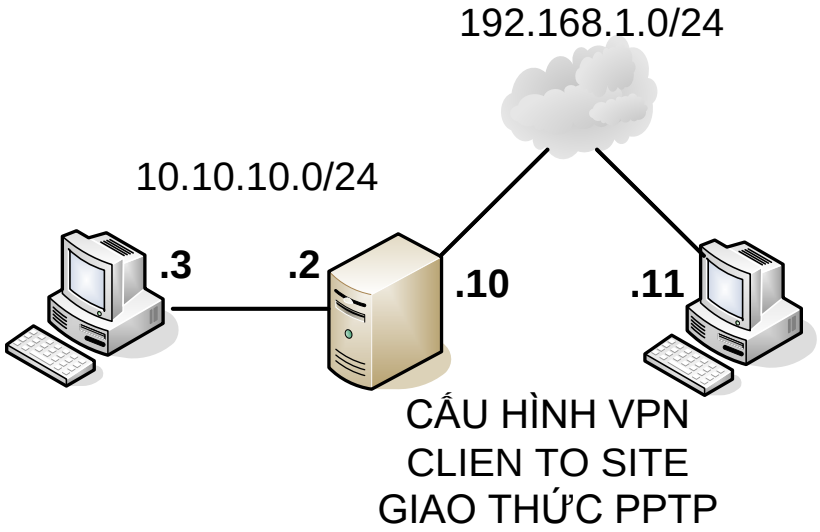
Point-to-Point Tunneling Protocol (PPTP): Giao thức PPTP là một sự mở rộng của giao thức PPP, nó đóng gói các frame PPP trong các IP datagram. Sau đó các IP Datagram được chuyển trên liên mạng IP như là Internet. PPP được tạo để sử dụng cho các kết nối TCP để bảo vệ đường hầm(tunnel). Sự thay đổi GRE được tóm lược các frame PPP được sử dụng cho đường hầm dữ liệu. Các frame PPP này có thể được nén hoặc mã hoá để đảm bảo an toàn. Các phương pháp xác thực tương tự được sử dụng bởi các kết nối PPP mà nó được sử dụng cho quá trình xác thực các tunnel PPP. Nó thừa kế quá trình nén và mã hoá các PPP các đơn vị dữ liệu từ PPP. Nó cũng có thể được sử dụng cho các mạng riêng LAN-to-LAN.

Bài tập thực hành VPN Client to Site dùng giao thức PPTP

Yêu cầu: Cài đặt, cấu hình cho máy client truy cập vào hệ thống bằng dịch vụ VPN client to site

Chuẩn bị:

- 2 máy PC cài win XP
- 1 máy PC cài win 2k3→VPN
- Đấu nối mô hình mạng



- Thiết lập địa chỉ IP

TÊN	CARD LAN	CARD INTERNET

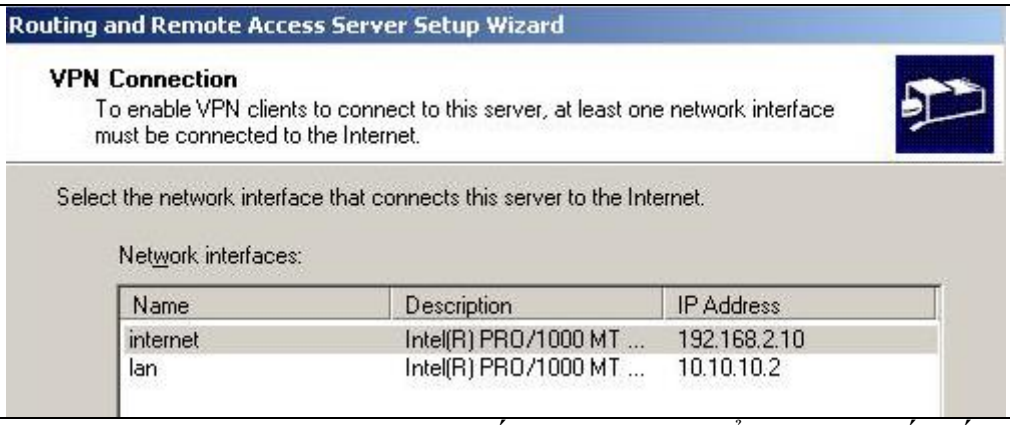
MÁY				
SERVER	IP	10.10.10.2	IP	192.168.2.10
	Subnetmask	255.255.255.0	Subnetmask	255.255.255.0
	Getway	Để trống	Getway	192.168.2.1
	Preferred DNS server:	10.10.10.2	Preferred DNS server:	8.8.8.8
	Alternate DNS server:	Để trống	Alternate DNS server:	8.8.4.4
PC1	IP	10.10.10.3		
	Subnetmask	255.255.255.0		
	Getway	10.10.10.2		
	Preferred DNS server:	10.10.10.2		
	Alternate DNS server:	Để trống		
VPN CLIENT			IP	192.168.2.11
			Subnetmask	255.255.255.0
			Getway	192.168.2.1
			Preferred DNS server:	8.8.8.8
			Alternate DNS server:	8.8.4.4

Thực hiện

Cài đặt và cấu hình

Bước 1: Vào Star → Administrative → khởi động dịch vụ Routing and remote access→ Click phải chuột lên "server" → Configure … →Next

Bước 2: Chọn Remote access (dial-up or VPN)→ VPN → Next→ card kết nối Internet → bỏ check Enable … →Next


Routing and Remote Access Server Setup Wizard
VPN Connection
To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.
Select the network interface that connects this server to the Internet.
Network interfaces:
Name
Description
IP Address
internet
Intel(R) PRO/1000 MT ...
192.168.2.10
lan
Intel(R) PRO/1000 MT ...
10.10.10.2

Bước 3: Chọn From a …. → New→ Cấp dãy địa chỉ để khi user kết nối VPN vào sẽ nhận dãy IP này và chú ý phải nhập cùng lớp mạng với Card Lan của máy server.

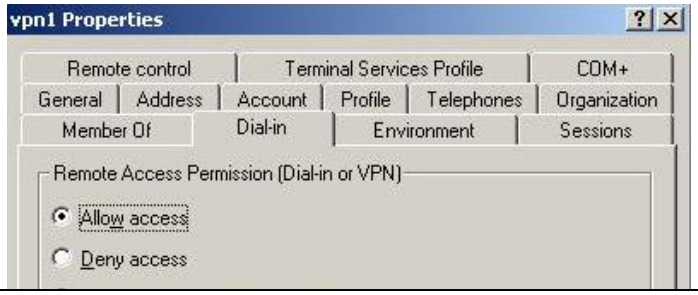
VD: cấp dãy IP từ 100 → 150 thì ta gõ

10.10.10.10 – 10.10.10.150 → OK

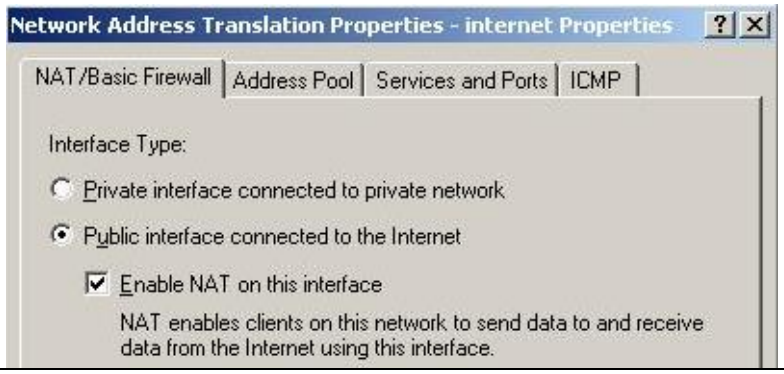
New Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
10 . 10 . 10 . 100
End IP address:
10 . 10 . 10 . 150
Number of addresses:
51
OK
Cancel

Chọn Next→ No, …. → Next→ Finish → OK

Bước 4: Trên máy server tạo một user để kết nối VPN→ Cấp quyền cho phép user kết nối VPN

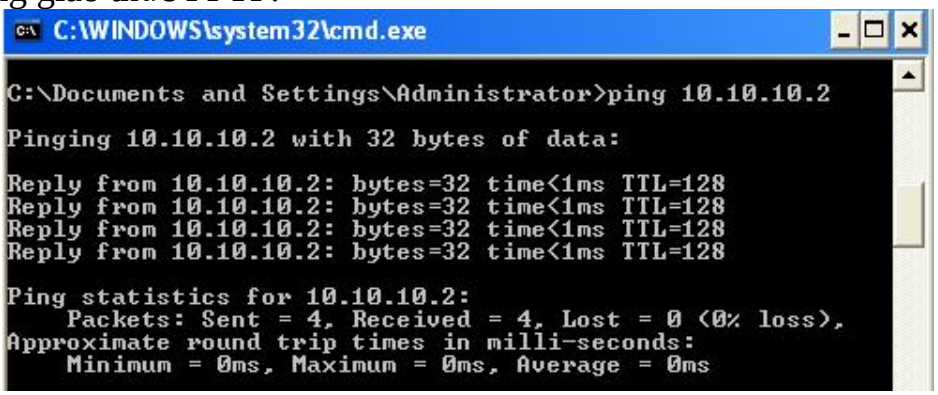


Bước 5: Chọn Card "internet" →Check chọn Public interface ,, check chọn Enable NAT …→ OK


Network Address Translation Properties - internet Properties
NAT/Basic Firewall
Address Pool
Services and Ports
ICMP
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.

Bước 6: Trên máy VPN CLIENT → tạo kết nối VPN
Khởi động Network Connect lên → chọn Create a new connection →Next

Bước 7: Ping thử đến địa chỉ card Lan của máy server, địa chỉ card Lan của máy PC1 . nhận xét thấy thành công. Như vậy là cấu hình hoàn thành kết nối VPN bằng giao thức PPTP.


C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

3.Mô hình VPN Client to Site dùng giao thức L2TP/IPSec

Mục tiêu: Cài đặt, cấu hình được mô hình client to site
Giao thức Layer 2 Tunneling Protocol (L2TP)

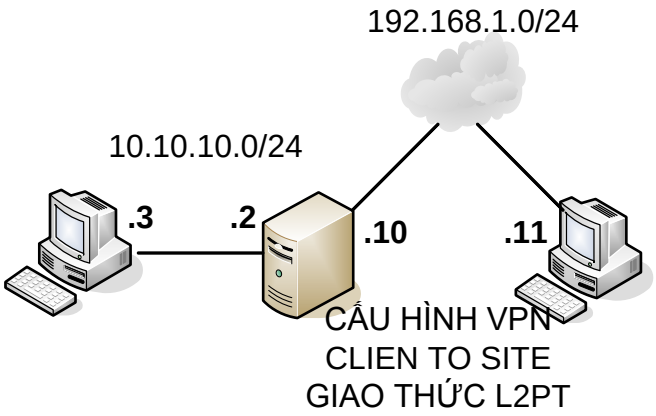
Giao thức L2TP cung cấp một tunnel giữa các domain không có tin cậy trong một mạng tương tự giao thức PPTP. Cả hai giao thức này cung cấp việc bắt đầu đóng gói dữ liệu sử dụng PPP. Giao thức L2TP cấu thành từ PPTP và L2F(Layer 2 Forwarding). Nó đóng gói các frame PPP, nó có thể được gửi trên IP, frame relay, X.25 hoặc mạng ATM. L2TP có thể được sử dụng như giao thức tunnel trên Internet nếu nó sử dụng IP như là truyền tải của nó. Sự bảo vệ Tunnel L2TP sử dụng UDP và một dãy các thông điệp điều khiển L2TP.

Bài tập thực hành VPN Client to Site dùng giao thức L2TP/IPSec

Yêu c ầu: Cài đặt, cấu hình cho máy client truy cập vào hệ thống bằng dịch vụ VPN client to site dùng giao thức L2TP/IPSec

Chuẩn bị

- 2 máy PC cài win XP
- 1 máy PC cài win 2k3→VPN
- Đấu nối mô hình mạng



- Thiết lập địa chỉ IP

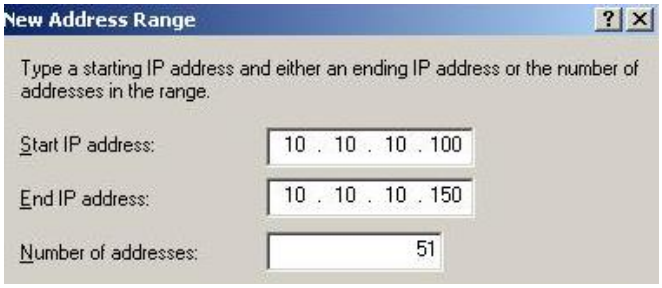
TÊN MÁY	CARD LAN		CARD INTERNET	
SERVER	IP	10.10.10.2	IP	192.168.2.10
	Subnetmask	255.255.255.0	Subnetmask	255.255.255.0
	Getway	Để trống	Getway	192.168.2.1
	Preferred DNS server:	10.10.10.2	Preferred DNS server:	8.8.8.8
	Alternate DNS server:	Để trống	Alternate DNS server:	8.8.4.4
PC1	IP	10.10.10.3		
	Subnetmask	255.255.255.0		
	Getway	10.10.10.2		
	Preferred DNS server:	10.10.10.2		
	Alternate DNS server:	Để trống		
VPN CLIENT			IP	192.168.2.11
			Subnetmask	255.255.255.0
			Getway	192.168.2.1
			Preferred DNS server:	8.8.8.8
			Alternate DNS server:	8.8.4.4

Thực hiện

Cài đặt và cấu hình

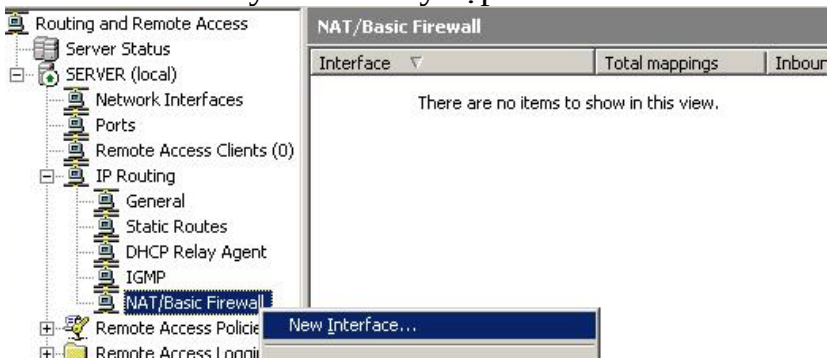
Bước 1: Vào Star → Administrative → khởi động dịch vụ Routing and remote access→ Click phải chuột lên "server" → Configure … →Next

Bước 2: Chọn Remote access (dial-up or VPN)→ VPN → Next→ card kết nối Internet → bỏ check Enable … →Next→ From a …. Next → Cấp dãy địa chỉ để khi user kết nối VPN


New Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address: 10 . 10 . 10 . 100
End IP address: 10 . 10 . 10 . 150
Number of addresses: 51

Chọn No, …. → Next→ Finish → OK

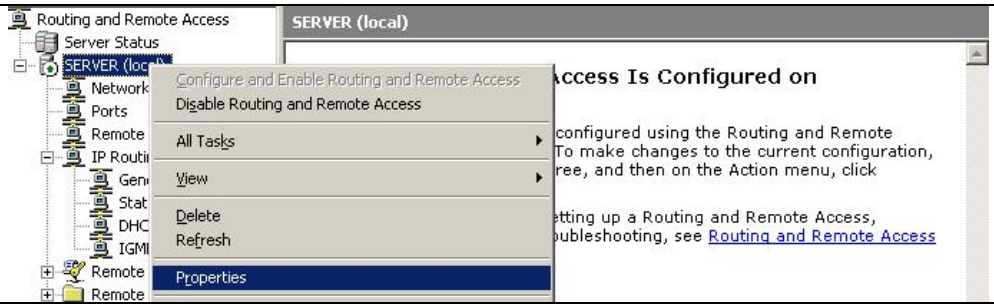
Bước 3: tạo một user để kết nối VPN→ Cấp quyền cho phép user kết nối VPN → Cấu hình NAT để cho máy Client truy cập Internet



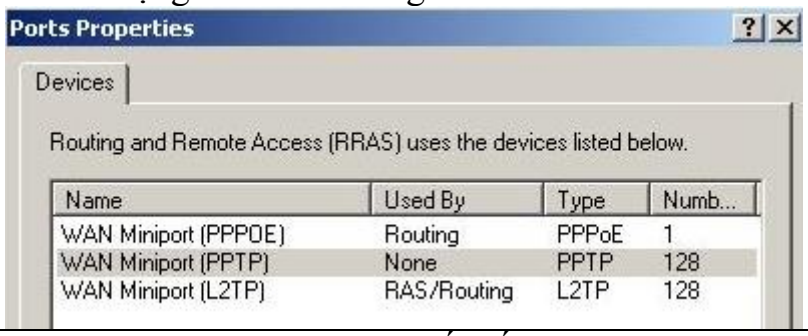
Làm tương tự như VPN Client to Site dùng giao thức PPTP

Bước 4: Cấu hình kết nối VPN bằng giao thức L2PT/IPSEC

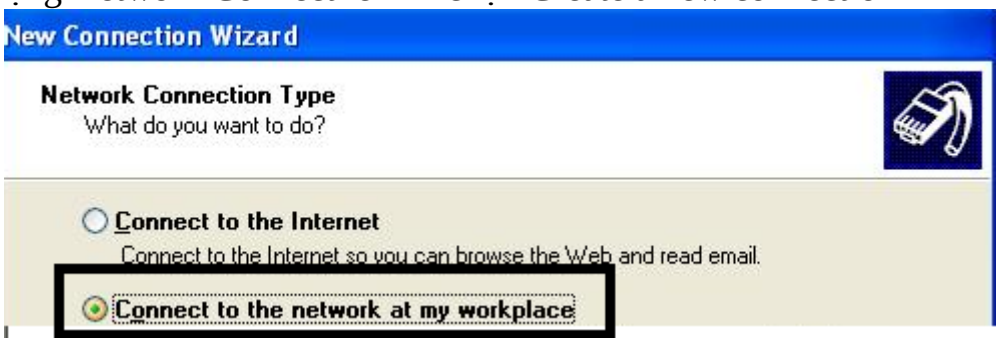
Click phải chuột lên "server" → properties



Bước 5: Bỏ check 2 mục remote access và Deman-dial → OK
Như vậy PPTP đã ở trạng thái "None" nghĩa là đã tắt.

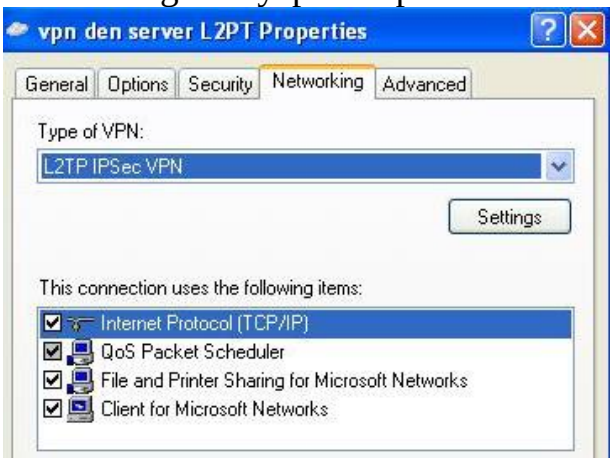


Bước 6: Trên máy VPN CLIENT → tạo kết nối VPN
Khởi động Network Connect lên → chọn Create a new connection


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace

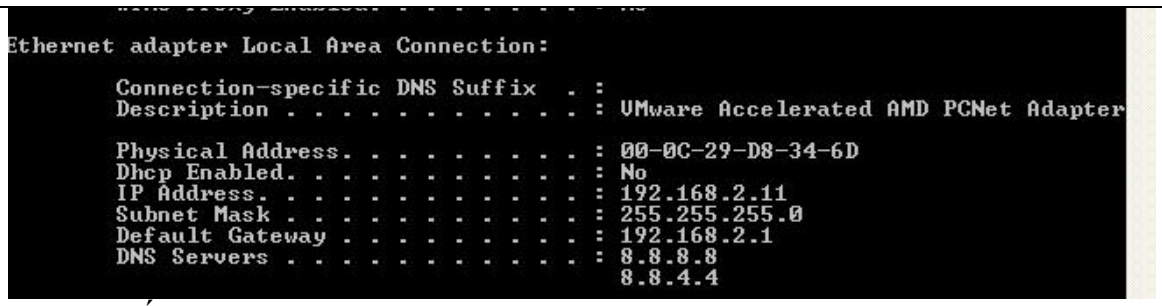
Chọn Vitual private Network connection → Next→ Nhập địa chỉ của máy làm VPN SERVER→Next→ Finish

Bước 7: Chọn Tab Networking → Tyepe of vpn → L2PT IPSEC VPN

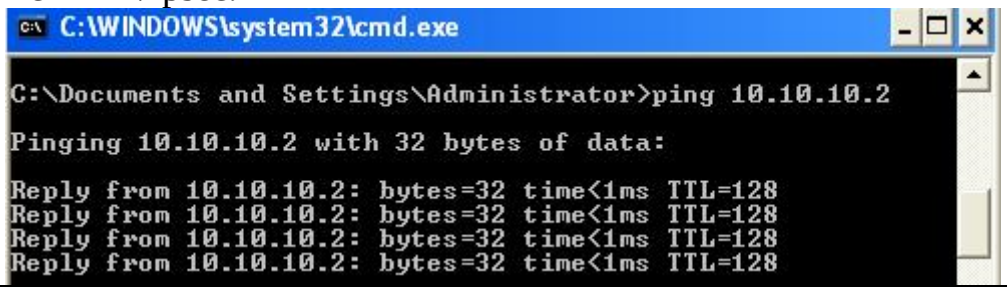


Tại tab Security → Ipsec seting

Bước 8: Kiểm tra xem máy server cấp đúng dãy IP đã tạo ban đầu hay chưa.
Vào CMD gõ lệnh: ipconfig /all


Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-D8-34-6D
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.2.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
DNS Servers . . . . . : 8.8.8.8
8.8.4.4

Ping thử đến địa chỉ card Lan của máy server, địa chỉ card Lan của máy PC1 . nhận xét thấy thành công. Như vậy là cấu hình hoàn thành kết nối VPN bằng giao thức L2PT/Ipsec.

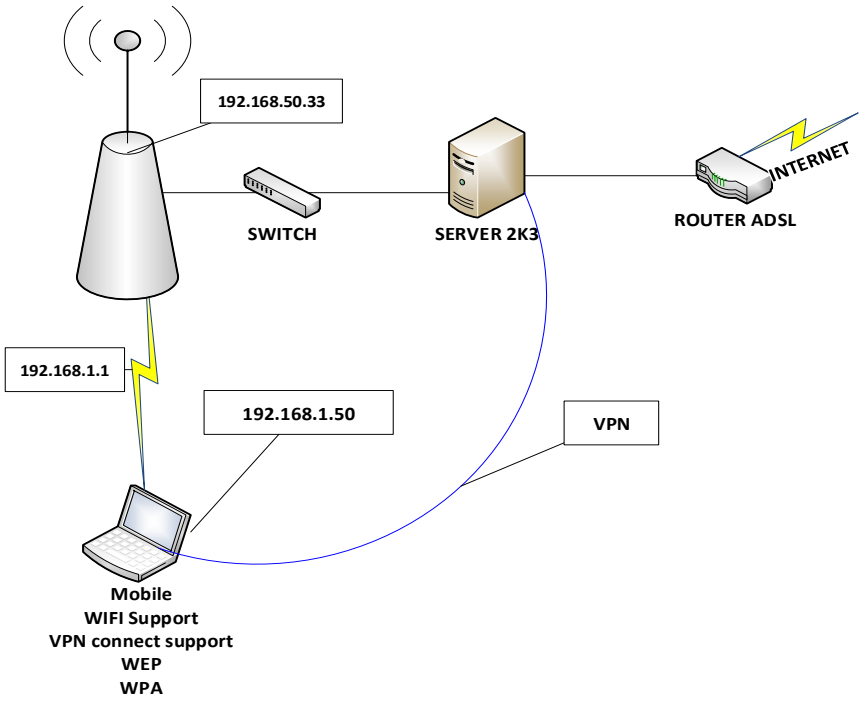

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128

4.Mô hình VPN Client to Site dùng chương trình No-IP

VPN Client to Site cho phép chúng ta truy cập giữa các site hay các client đến site thông qua môi trường internet. Kết hợp với tường lửa thì khi đó sẽ đảm bảo độ tin cậy cũng như an toàn dữ liệu thông qua một đường pipe (ống) riêng ảo được tạo ra trên môi trường internet của công nghệ VPN

Bài tập thực hành**:** MAX Secure Wi-Fi với VPN của Windows 2003 với Mô hình mạng như sau

Mô hình mạng



Yêu cầu

- Cấu hình mã hóa gói tin từ Laptop tới Access Point sử dụng WPA2-Personal
- Truy cập vào Access Point để bắt đầu cấu hình, sau khi truy cập vào Access Point qua giao diện Web, cấu hình địa chỉ IP cho Access Point.
- Port Internet trên Access Point, đặt địa chỉ là: 192.168.50.33, các thông số thiết lập như trên
- Địa chỉ IP làm Gateway các thiết bị Wi-Fi tôi đặt: 192.168.1.1
- Địa chỉ IP gán cho các thiết bị kết nối tới Access Point là giải:192.168.1.0/24

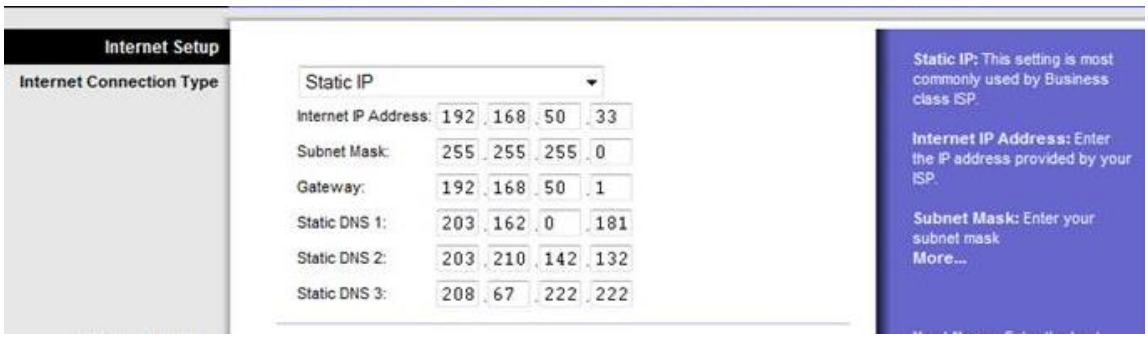
Chuẩn bị

- Sử dụng Access Point của Linksys
- Thiết bị bao gồm: 1 Port ra Internet, 4 Port LAN
- Cắm dây từ Switch vào Port Internet
- 1 máy PC cài win2k3
- 1 máy laptop
- 1 switch
- 1 router kết nối internet
- 3 sợi cáp bấm thẳng

Thực hiện

Cấu hình trên Access Point và kết nối

Bước 1: Cấu hình tính năng Security cho các kết nối Wi-Fi

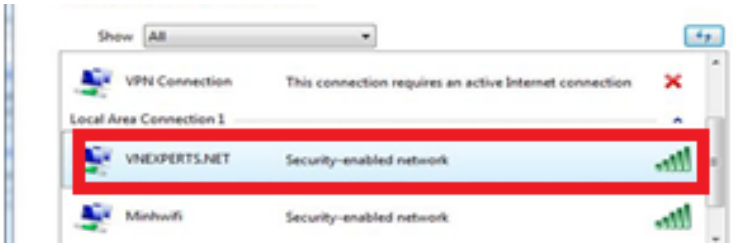

Internet Setup
Internet Connection Type
Static IP
Internet IP Address: 192 . 168 . 50 . 33
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 50 . 1
Static DNS 1: 203 . 162 . 0 . 181
Static DNS 2: 203 . 210 . 142 . 132
Static DNS 3: 208 . 67 . 222 . 222
Static IP: This setting is most commonly used by Business class ISP.
Internet IP Address: Enter the IP address provided by your ISP.
Subnet Mask: Enter your subnet mask
More...

Bước 2: Chọn Security Mode là: WPA2 Personal→ Chọn thuật toán mã hóa cho giao thức WPA là: TKIP+AES→Key khi các thiết bị muốn kết nối tới mạng Wireless này là: vnexperts.net

Wireless Security
Security Mode: WPA2 Personal
WPA Algorithms: TKIP+AES
WPA Shared Key: vnexperts.net
Group Key Renewal: 3600 seconds
Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...

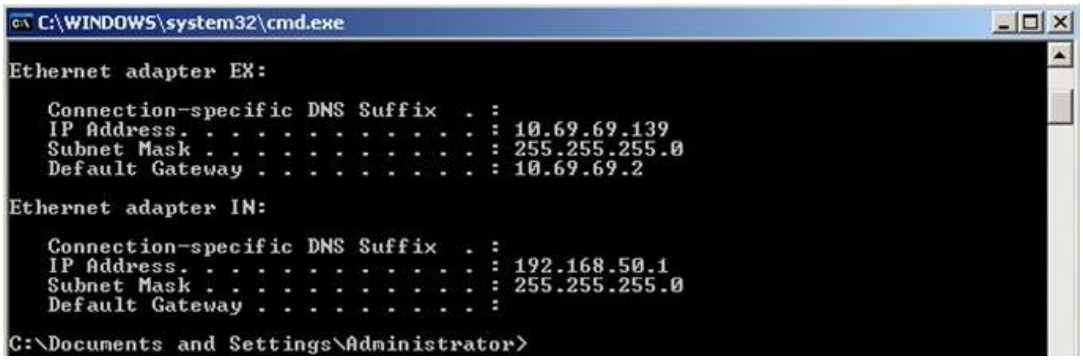
SSID chọn VNEXPERTS.NET→Save toàn bộ các thiết lập

Bước 3: Dùng chính công cụ trên Windows tìm kiếm các SSID của mạng Wireless. Thấy có mạng có SSID là VNEXPERTS.NET nhấn Connect gõ key như vừa rồi vào là hoàn thành kết nối Wireless



Cấu hình Enable tính năng VPN trên máy chủ Windows Server 2003.

Bước 1: Đặt địa chỉ IP cho hai card mạng của máy chủ

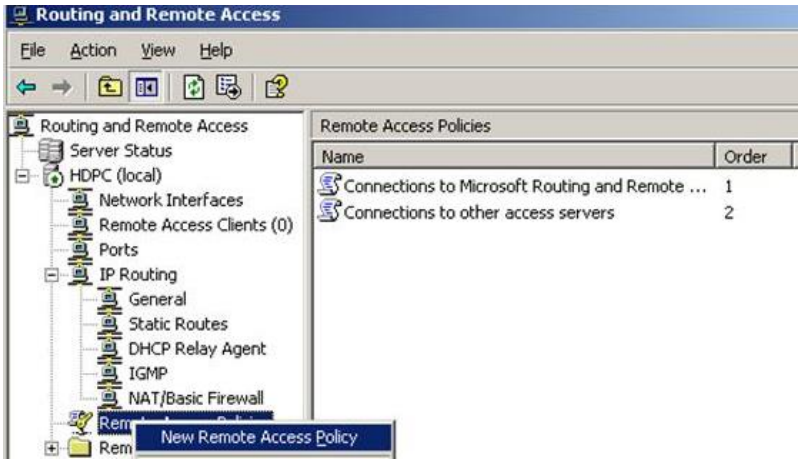

C:\WINDOWS\system32\cmd.exe
Ethernet adapter EX:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.69.69.139
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.69.69.2
Ethernet adapter IN:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.50.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
C:\Documents and Settings\Administrator>

Bước 2: Start →Administrative tools →Routing and Remote Access →Chuột phải chọn Enable and …→Next tới cửa sổ tiếp theo chọn Custom Configuration

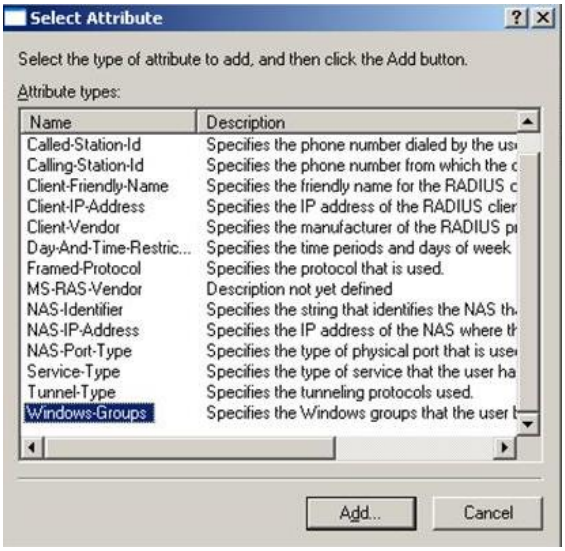
Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)

Bước 3: Tạo User và Group cho phép truy cập VPN→Sau đó tạo một Group với tên VPN rồi Add user vnexperts.net vào group→Tạo Remote Access Policy cho phép may chủ thành VPN Server→Chuột phải vào Remote Access

Policy chọn New Remote Access Policy



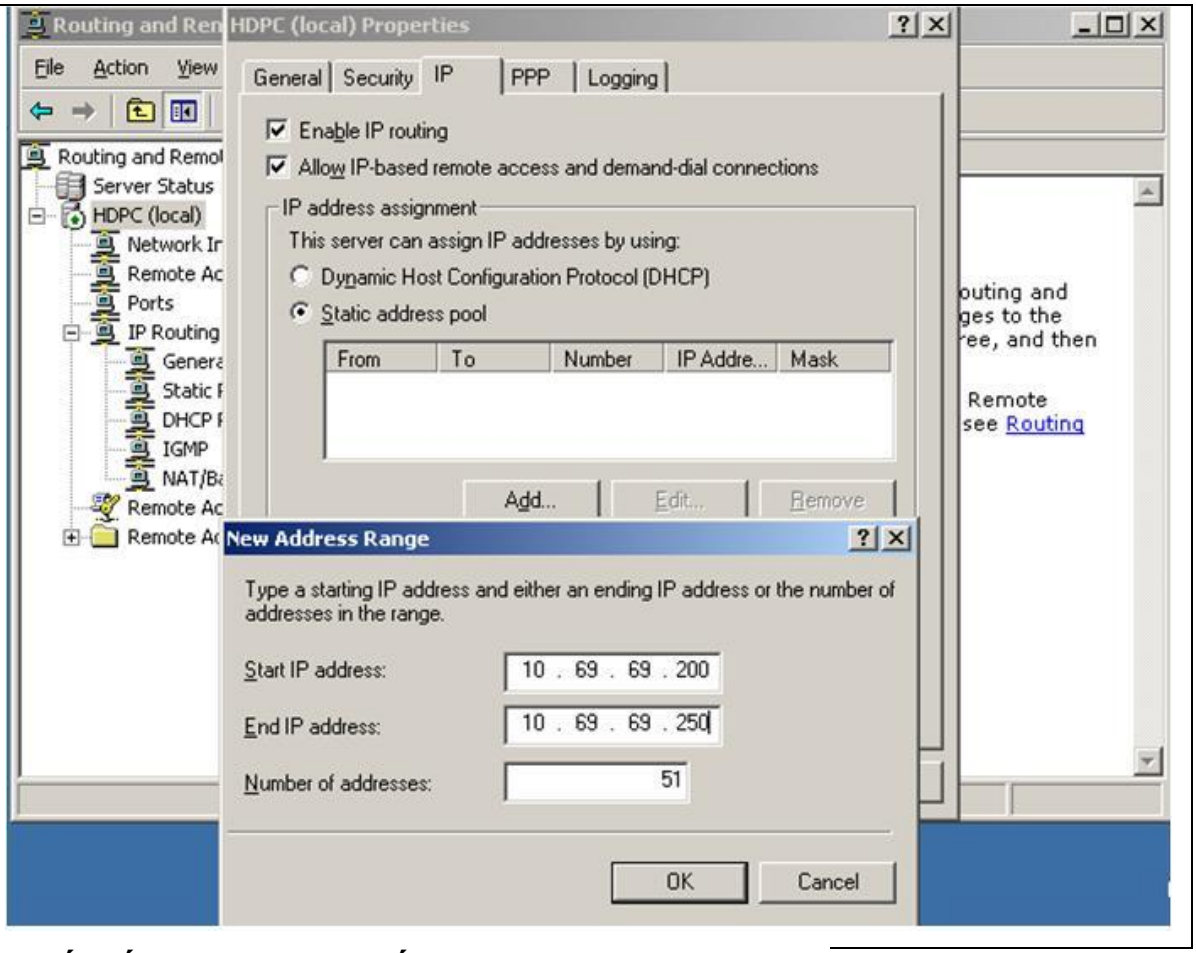
Bước 4: Chọn Custome rồi gõ tên của Remote Access Policy→Next→Add rồi chọn tới Windows Group



Bước 5: Add Group VPN cho phép truy cập→Nhấn OK để tiếp tục quá trình→Grant cho phép truy cập nhấn Next rồi Finish

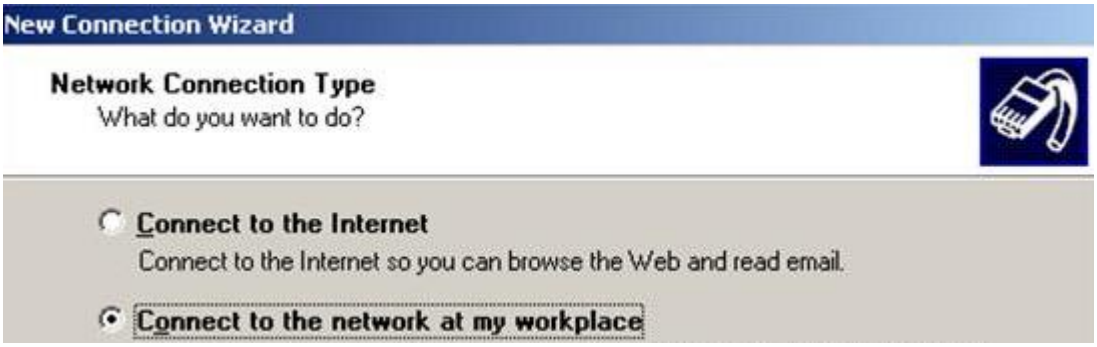
Routing and Remote Access
File Action View Help
New Remote Access Policy Wizard
Permissions
A remote access policy can either grant or deny access to users who match the specified conditions.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission

Bước 6: Gán địa chỉ IP cho những kết nối VPN tới→Chuột phải máy chủ chọn Properties→Chuyển sang Tab IP chọn Options Static Address Pool→Nhấn Add để gán dải địa chỉ IP cho các kết nối VPN


Routing and Ren
HDPC (local) Properties
File Action View
General Security IP PPP Logging
Enable IP routing
Allow IP-based remote access and demand-dial connections
IP address assignment
This server can assign IP addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From To Number IP Addre... Mask
Add... Edit... Remove
Routing and Remot
Server Status
HDPC (local)
Ports
IP Routing
IGMP
Remote Ac
New Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address: 10 . 69 . 69 . 200
End IP address: 10 . 69 . 69 . 250
Number of addresses: 51
OK Cancel
outing and
ges to the
ree, and then
Remote
see Routing

Tạo kết nối VPN từ các thiết bị truy cập qua Wireless.

Bước 1: Start →Control Panel →Network Connections →Chọn "New Connection Wirard"→kết nối VPN, nhấn Next để tiếp tục quá trình

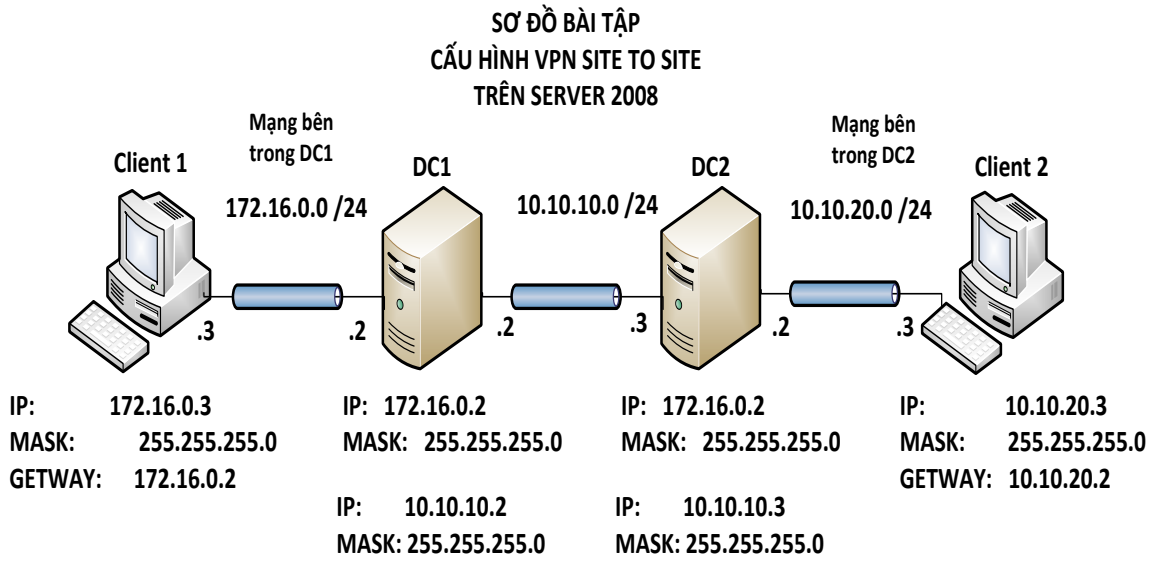

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace

Bước 2: Nhấn dúp vào kết nối tôi vừa tạo gõ User "vnexperts.net" → 192.168.50.1 →Connect

5.Mô hình VPN Site to Site

Site to site: Hệ thống này thường được sử dụng giữa các chi nhánh của 1 tổ chức hoặc mạng lưới công ty nào đó. Tại đây, bạn phải sử dụng 1 thiết bị hỗ trợ VPN như Cisco ASA hoặc router của Cisco. Người sử dụng có thể cấu hình cả 2 thiết bị để thiết lập hệ thống tunnel lẫn nhau, và toàn bộ mô hình của công ty hoặc văn phòng sẽ sử dụng qua tunnel tại cùng 1 thời điểm (trong khi các kết nối truy cập VPN từ xa chỉ có thể được thực hiện trên PC đã được thiết lập tunnel sẵn) để truy cập tới các nguồn tài nguyên trong cùng 1 hệ thống.

Bài tập thực hành**:** cho mô hình mạng như sau



Yêu cầu:Cài đặt, cấu hình VPN site to site trên mô hình mạng

Chuẩn bị

- 2 máy PC cài win2k8
- 2 máy PC cài win7
- 3 switch
- 4 sợi cáp mạng bấm thẳng
- Đấu nối mô hình

Thực hiện

Trên DC 1

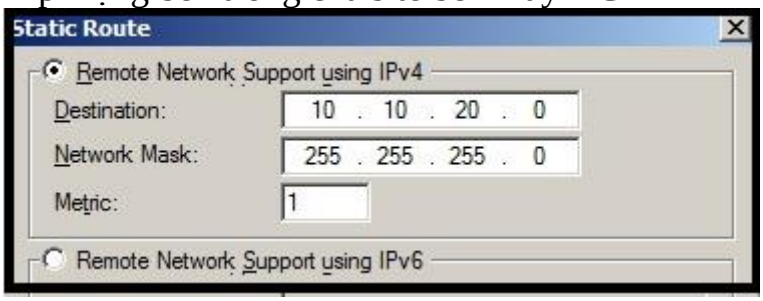
Bước 1: Trên máy DC1 tạo user u2 pass: 123, máy DC2 tạo u1 pass: 123 Trên DC 1 cài đặt routing and remote access Vào start →administrative Tools → server manager → Roles → Add Roles

Next→Next→ Network policy …→ Next→ chọn Routing and … → Next → Install→ Close

Bước 2: Click phải chuột lên Network Interfaces → New Demand-dial Interface

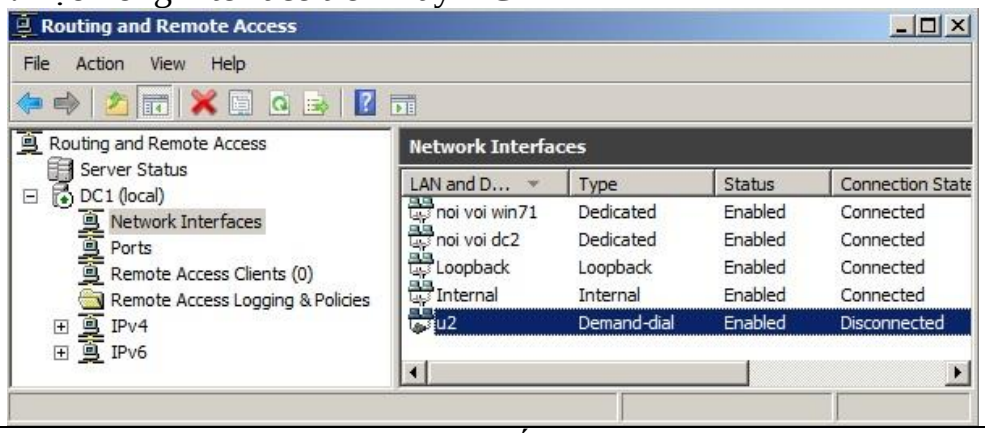
Nhập user name trên DC 1 vừa tạo→ chọn kết nối VPN

Bước 3: Nhập lớp mạng bên trong của site bên máy DC2

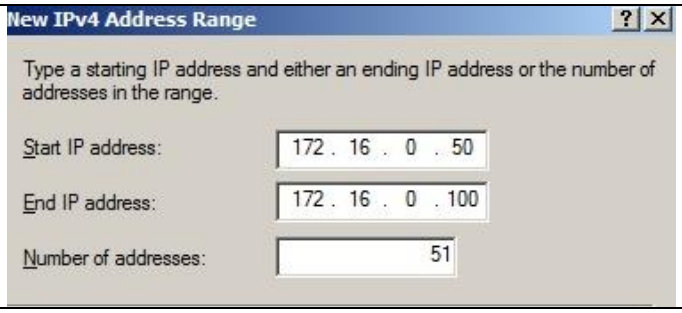

Static Route
Remote Network Support using IPv4
Destination: 10 . 10 . 20 . 0
Network Mask: 255 . 255 . 255 . 0
Metric: 1
Remote Network Support using IPv6

Chọn Next→ pass của u2→ user name và password của máy DC2 đã tạo ban đầu→ Finsh→ Yes

Bước 4: Tạo xong interface trên máy DC1



Bước 5: Tạo dãy IP →Static → Add→ Cấp cùng dãy IP bên trong của Máy DC1→OK→ restart

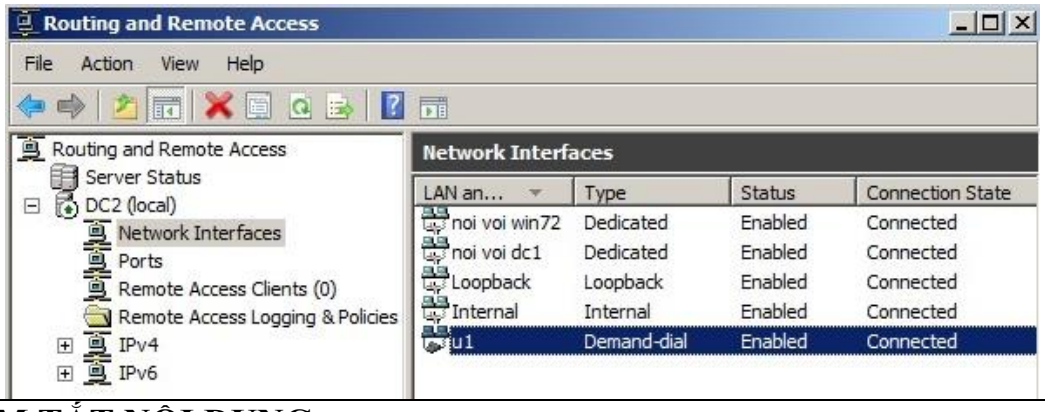

New IPv4 Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
172 . 16 . 0 . 50
End IP address:
172 . 16 . 0 . 100
Number of addresses:
51

Bước 6: Cấu hình trên DC2 → Routing and remote acess
Click phải chuột lên DC2 → configure … →

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
DC2 (local)
Routing and Remote Access
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access

Next→ Administrative Tools → Next→ Chọn Custom configure → Next→ Finsh → Start services

Bước 7: TạoNew Demand-dial Interface→ tạo VPN→ Kết nối



6.TÓM TẮT NỘI DUNG

- Mạng VPN truy cập từ xa (Remote Access VPN), không cần sự hỗ trợ của nhân viên mạng vì quá trình kết nối được Internet Service Provider viết tắt ISP thực hiện.
- Mạng VPN cục bộ (Intranet), sử dụng kỹ thuật đường hầm thông qua internet kết hợp với công nghệ chuyển mạch tốc độ nhanh.
- Mạng VPN mở rộng (Extranet), được xây dựng dựa trên mạng internet có nhiều cơ hội cung cấp dịch vụ và chọn lựa giải pháp phú hợp với mô hình mạng. Khả năng bảo mật thông tin cao
- Với công nghệ VPN sẽ làm tăng khả năng khai thác thông tin mọi lúc, mọi nơi và đảm bảo khả năng an toàn bảo mật trong quá trình khai thác đó.

7.CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày các mô hình VPN.

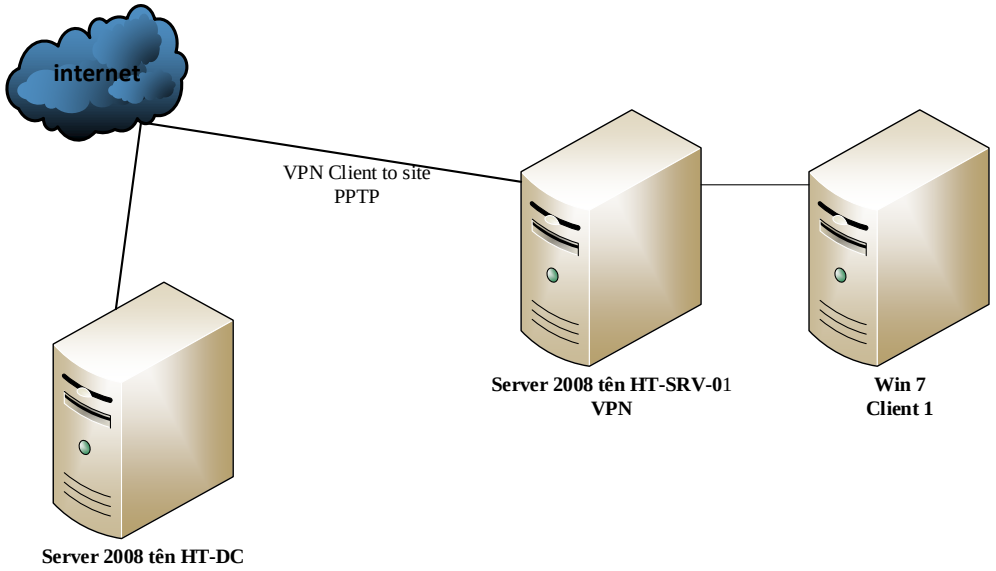
Câu 2: Trình bày ưu điểm và nhược điểm của mạng VPN cục bộ (Intranet VPN)

Cẫu 3: Trình bày ưu điểm và nhược điểm của mạng VPN mở rộng (Extranet VPN)

Câu 4: Trình bày yêu cầu phần cứng, phần mềm khi thiết lập mô hình VPN server trên windows server 2003 và 2008

BÀI TẬP

Bài tập 1: Cho mô hình mạng



Yêu c ầu: Cài đặt, cấu hình VPN Client to site (Client Access) với giao thức PPTP trên win2k8

Chuẩn bị

- 1 máy windows server 2008 tên HT-DC đã nâng cấp lên DC với domain tuancdvs.vn
- 1 máy windows server 2008 tên HT-SRV-01 đã join vào domain dùng để cài đặt VPN Server.
- 1 máy Windows 7 tên Client1 dùng làm VPN Client.
- Thiết lập địa chỉ IP cho các máy

Hướng dẫn làm bài

1. Tạo User và cấp quyền VPN

B1:Tạo User để kết nối VPN

B2:Cấp quyền VPN cho user

2. Cài đặt và cấu hình dịch vụ RRAS

B1:Cài đặt dịch vụ Routing and Remote Access

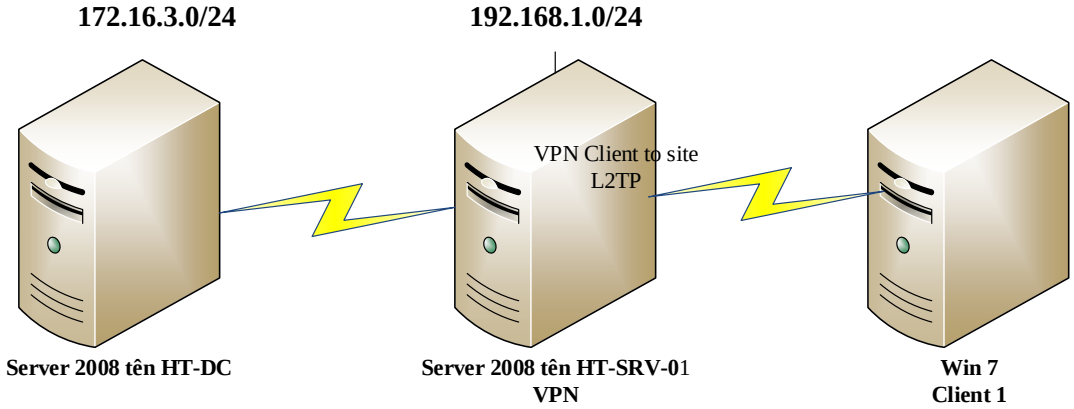
B2:Cấu hình VPN client to site

3. Tạo kết nối VPN trên VPN client

B1:TạoNew Demand-dial Interface→ tạo VPN→ Kết nối

B2: Thực hiện kết nối → kiểm tra

Bài tập 2: **Cho mô hình mạng**



Yêu cầu: Cài đặt, cấu hình VPN Client to site sử dụng giao thức L2TP Preshared Key trên win2k8

Chuẩn bị :

- 1 máy windows server 2008 tên HT-DC đã nâng cấp lên DC với domain tuancdvs.vn
- 1 máy windows server 2008 tên HT-SRV-01 đã join domain dùng để cài đặt VPN Server.
- 1 máy Windows 7 tên Client1 dùng làm VPN Client.
- Thiết lập địa chỉ IP cho các máy

Hướng dẫn làm bài

B1:Tạo User và cấp quyền VPN. Thực hiện trên máy HT-DC

B2:Cài đặt Routing and Remote Access RRAS. Thực hiện trên máy HT-SRV-01

B3:Cấu hình VPN client to site trên máy HT-SRV-01

B4:Cấu hình tạo key và sử dụng giao thức L2TP

B5:Tạo kết nối VPN và cấu hình VPN bằng giao thức L2TP

BÀI 9:PUBLISHING
Mã bài:MĐ 24-09

Thời gian: 13 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

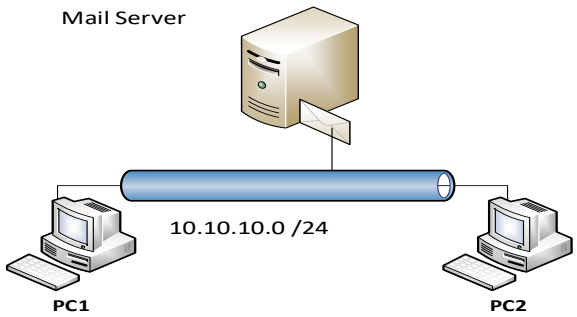
- Thiết lập được hệ thống sử dụng mail server;
- Cấu hình lọc được mail trong hệ thống;
- Thiết lập được web và FTP được chứng thực từ xa.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1.Cài Đặt hệ thống Mail Mdaemon và gửi mail qua lại

Chuẩn bị :

+ Máy PC cài Win2k3 và WinXP
+ 1 Switch
+ sợi dây cáp mạng
+ Đầu nối theo mô hình sau



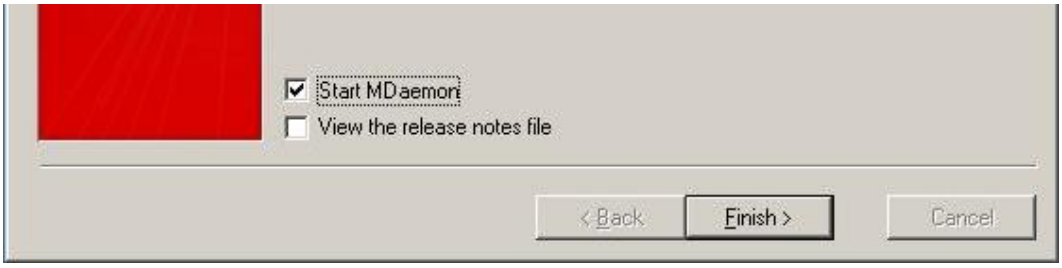
+ Đặt địa chỉ IP như sau:

Tên Máy	Card LAN
Mail Server	IP: 10.10.10.2 Subnet mask: 255.255.255.0 Preferred DNS server 10.10.10.2
PC1	IP: 10.10.10.3 Subnet mask: 255.255.255.0 Preferred DNS server 10.10.10.2
PC2	IP: 10.10.10.4 Subnet mask: 255.255.255.0 Preferred DNS server 10.10.10.2

Thực hiện

Cài đặt, cấu hình mail

Bước 1: Chạy File Setup.exe, màn hình Welcome To Mdeamon! Xuất hiện →Next→ I Agree→ Key đăng ký → Next→ tên Domain→ địa chỉ DNS



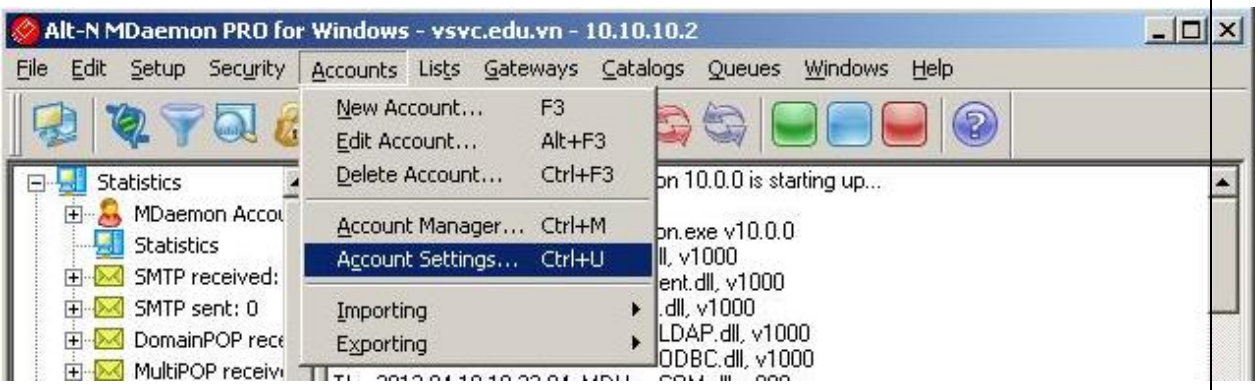
Chọn Finish , và Mdeamon bắt đầu khởi động

Bước 2: Sử dụng thêm số Port→Tại màn hình Mdeamon chọn Setup → Web & SyncML Services… hoặc nhấn (Ctrl+W)

Alt-N MDaemon PRO for Windows - vsvc.edu.vn - 10.10.10.2
File Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows Help
Default Domain / Servers... F2
Extra Domains... Alt+F2
Web & SyncML Services... Ctrl+W
Event Scheduling... Ctrl+E
Preferences... Ctrl+O
03: MDaemon 10.0.0 is starting up...
03: ---------
03: MDaemon.exe v10.0.0
03: NTUtil.dll, v1000
04: WorldClient.dll, v1000
04: MDUser.dll, v1000

WebAdmin → Run WebAdmin server using this TCP Port 80 → OK

Bước 3: Cấu hình bỏ chế độ password phức cho Mdeamon. Tại hộp thoại Mdeamon chọn Account Setting hoặc nhấn Ctrl+U

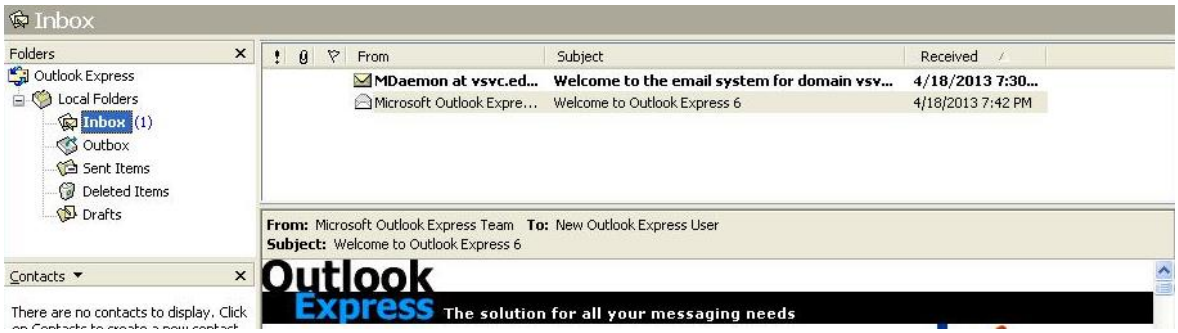


Bỏ check Requice strong passwords → OK→ Tạo tài khoản cho người dùng

Bước 4: Trên PC1 đăng nhập vào Domain và mở chương trình Outlook Express.Nhập tên hiển thị (User1) → Next→qt1.vsvc.edu.vn →Next

Chọn Finish kết thúc

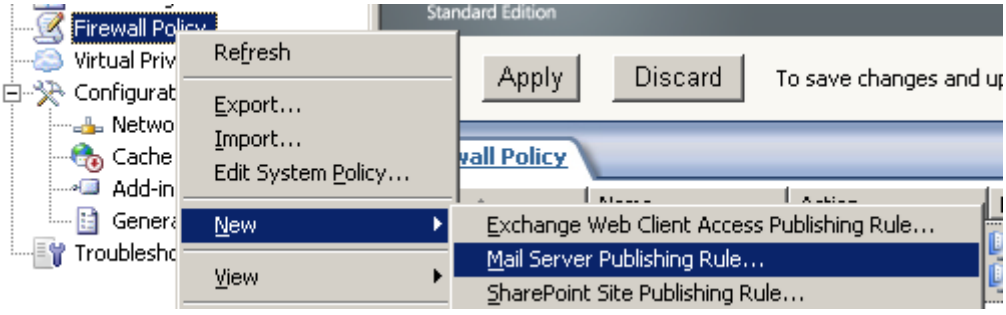
Bước 5: Đã nhận được mail Mdeamon gửi đến outlook express



2.Publishing Mail

Tạo rule lọc Mail

Bước 1: chuột phải Firewall Policy, chọn New rồi chọn Mail Server Publishing Rule.



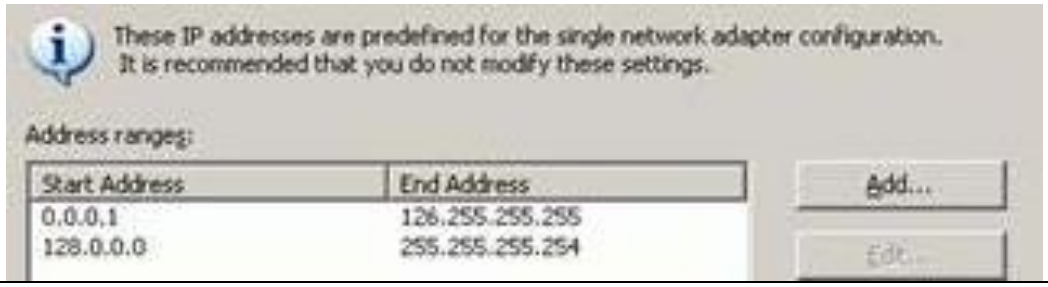
Bước 2:Check vào mục Client access: RPC, IMAP, POP3, SMTP→Next→ nhập IP Server Mail IP là 172.16.0.3, nhấn Next→ chọn External, nhấn Next.

3.Cấu hình Lọc mail

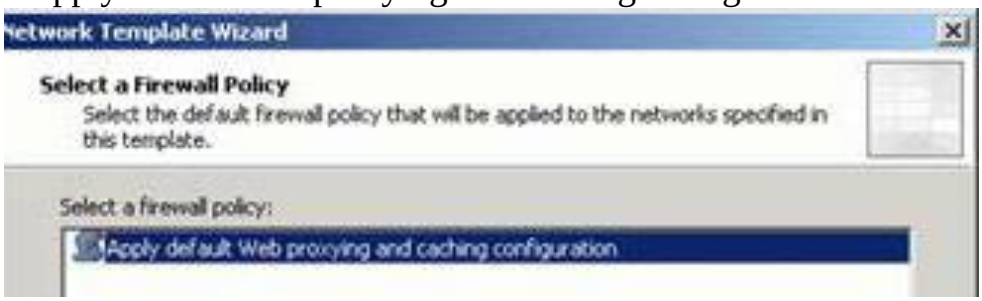
Cấu hình

Bước 1: Configuration → Networks→ Network Adapter→ Next→Next

Bước 2: Internal Network IP Addresses→Next



Bước 3: Apply default web proxying and caching configuration → Next.

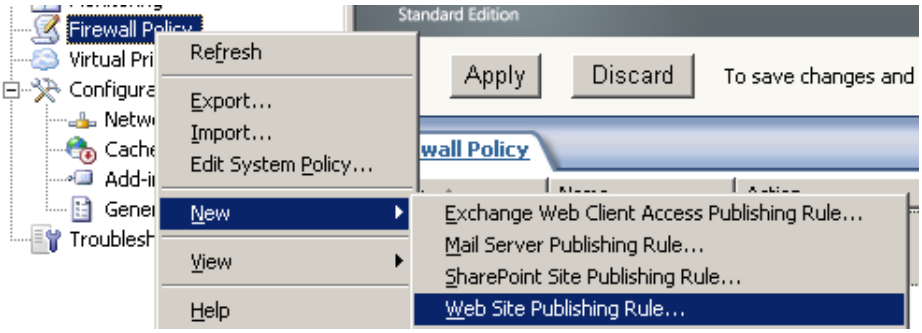

Network Template Wizard
Select a Firewall Policy
Select the default firewall policy that will be applied to the networks specified in this template.
Select a firewall policy:
Apply default Web proxying and caching configuration

Completing the Network Template Wizard→ Finish →OK

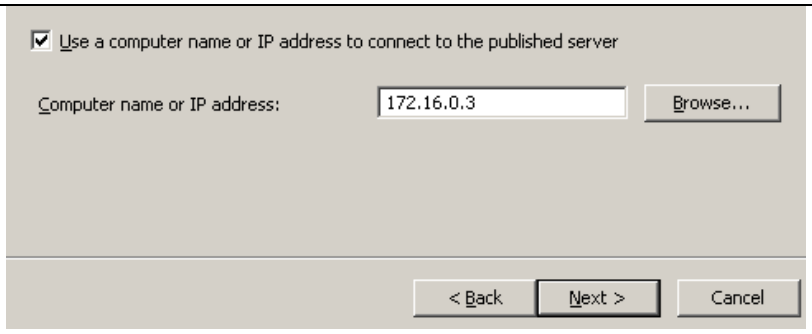
4.Publishing Web

Tạo rule

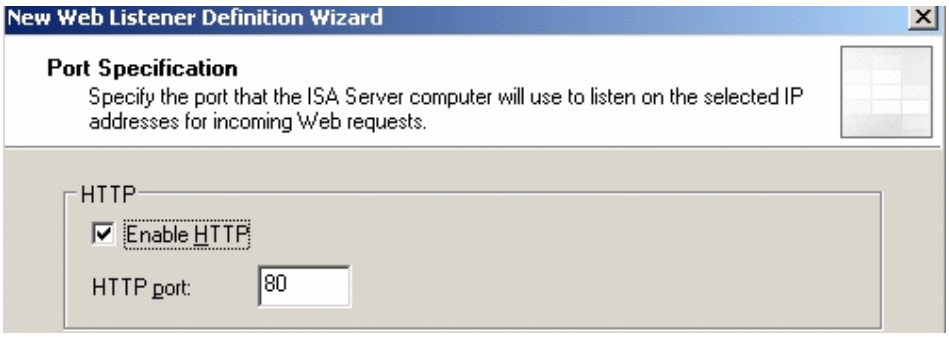
Bước 1: click chuột phải Firewall Policy, chọn New, chọn Web Server Publishing Rule→Next



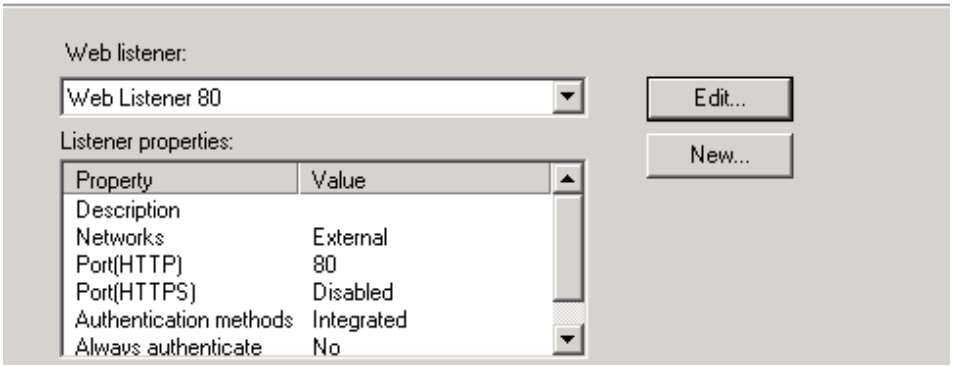
Bước 2: Chọn Alow→ Next→ IP WebServer 172.16.0.3→Next



Bước 3: IP addresses, đánh dấu chọn External→Next→ Enable HTTP port 80, →Next.


New Web Listener Definition Wizard
Port Specification
Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming Web requests.
HTTP
Enable HTTP
HTTP port:
80

Bước 4: Completing the New Web Listenner Wizard→Next.

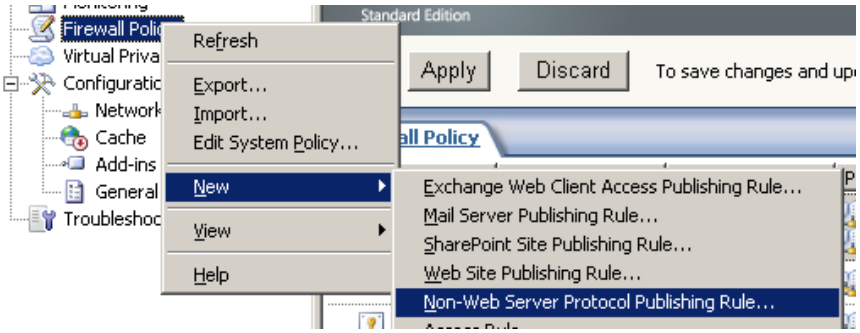


Chọn User Sets→ Finish

5.Publishing FTP

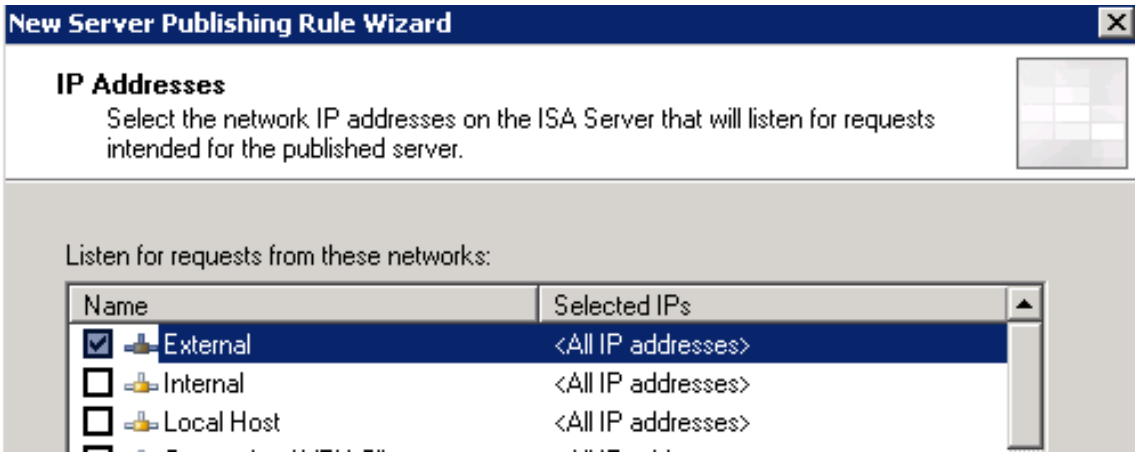
Tạo rule

Bước 1: Chọn Server Publishing Rule.



Next→ IP của FTP Server: 172.16.0.3→ Protocol là FTP Serevr→Next

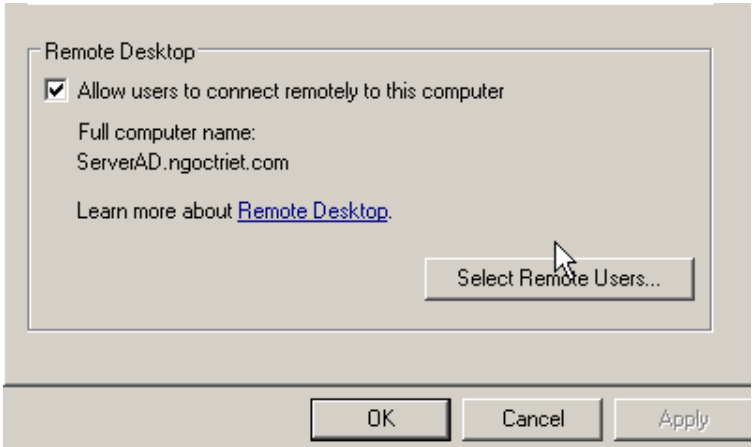
Bước 2: Hộp thoại IP Addresses, đánh dấu chon External, nhấn Next→ Finish



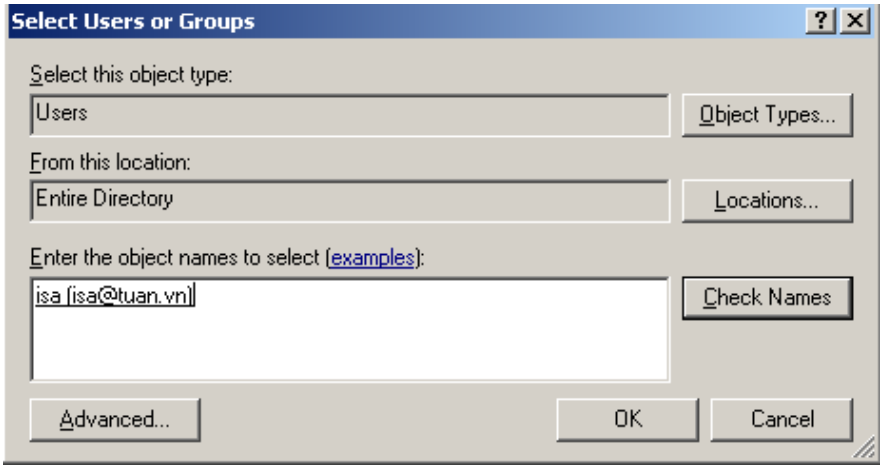
6.Publishing Terminal Services

Tạo kết nối

Bước 1: Chọn Select Remote Users→Add

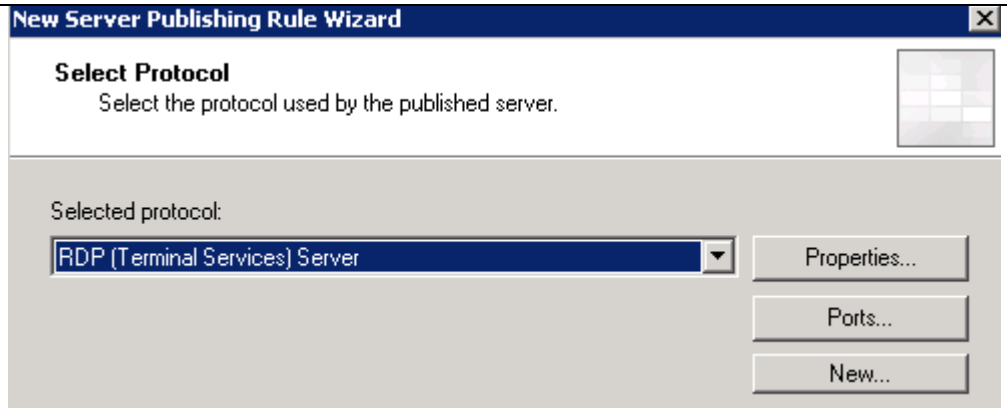


Bước 2: Hộp thoại Selected Users or Group, nhập vào tên user: kd1, chọn Check Names→Ok.



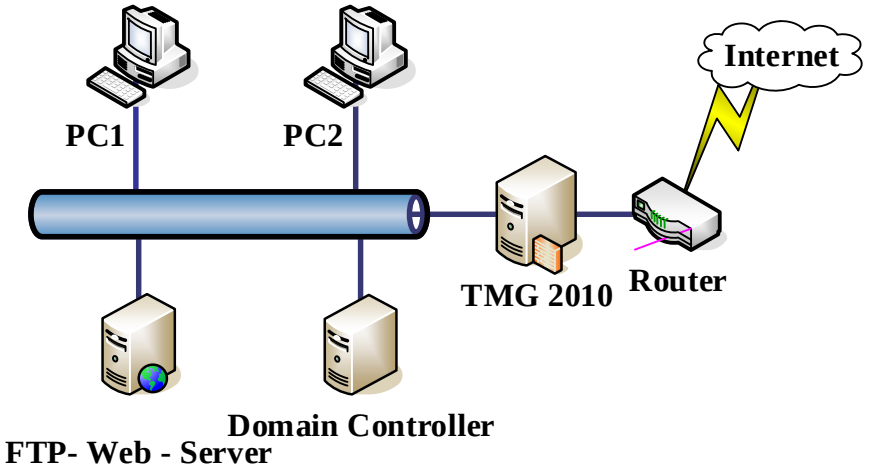
Click chuột phải Firewall Policy,chọn New, chọn Server Publishing Rules.

Bước 3: Đặt tên rule →Next→ RDP(Terminal Services)Server, chọn Next.



Chọn External→ Finish

Bài tập: Cho mô hình mạng



Yêu cầu:

Câu 1

- Hãy xây dựng một Domain với tên XXX.com (trong đó XXX là các chữ cái đầu của tên thí sinh)
- PC1, PC2 và ISA Server gia nhập vào Domain
- Cài đặt TMG 2010 Server trên máy TMG Server

Câu 2.

- Hãy tạo các tài khoản người dùng miền NV1, NV2, NV3 với mật khẩu đơn giản 12345
- Yêu cầu các máy tính trong mạng ra được Internet thông qua máy **TMG Server**
- Tạo Rule cho phép tài khoản NV3 được phép truy cấp Internet không hạn chế
- Tạo Rule cấm nhóm NV1, NV2 không được truy cập Internet trong giờ hành chính
- Thực hiện chuyển hướng trang Web http://nhatnghe.com về trang http://google.com.vn

- Cài đặt phần mềm Bandwidth Splitter để quản lý băng thông cho các tài khoản
- Thực hiện ưu tiên băng thông cho NV3 gấp đôi băng thông các tài khoản còn lại (dựa trên băng thông của đường truyền Internet để thực hiện việc này)
- Publish Web, FTP để các người dùng trong mạng, ngoài mạng có thể truy cập được

Chuẩn bị:

- 1 máy PC cài wn2k8 → TMG 2010
- 1 máy PC cài wn2k8 → DC
- 1 máy PC cài wn2k8 → FTP-Web Server
- 2 máy PC cài wn7 → Client
- 1 switch
- 1 router intenet
- 4 sợi cáp bấm thẳng
- 1 sợi cáp bấm chéo

Thực hiện:

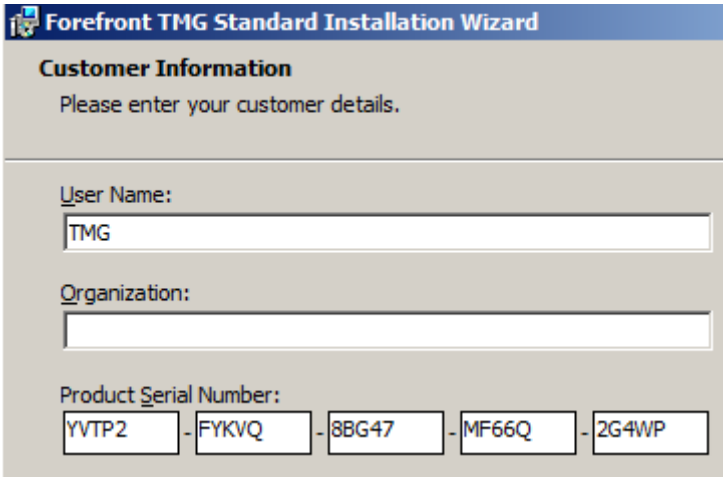
CÂU 1

Xây dựng một Domain (*xem lại QTM1*)

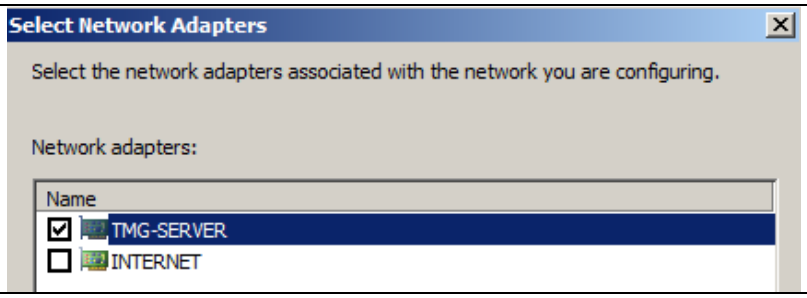
PC1, PC2 và TMG2010 Server gia nhập vào Domain *(xem lại QTM1)*

Cài đặt TMG 2010

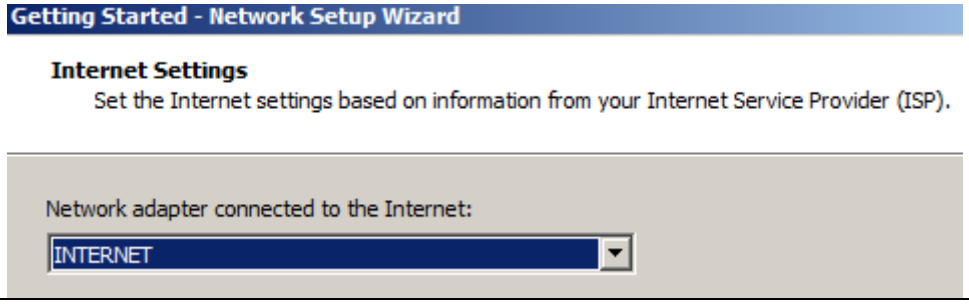
Bước 1: Run Preparation Tool→Next→ Tích vào accept the tems of the License Agreements → Next→ đặt tên →Next



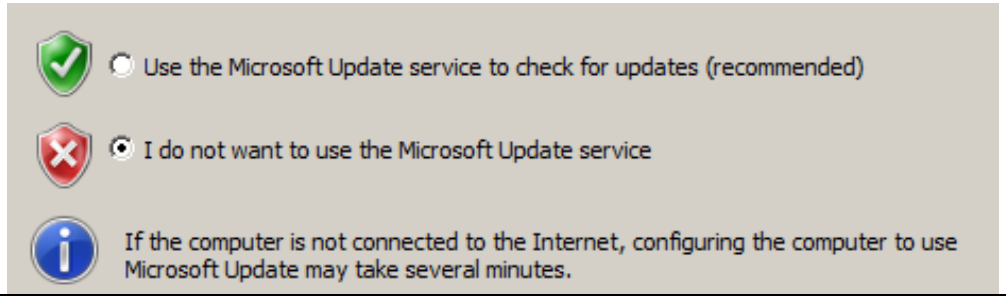
Bước 2: Tích vào Card TMG-SERVER → OK → OK→ Next → Install→ Finish



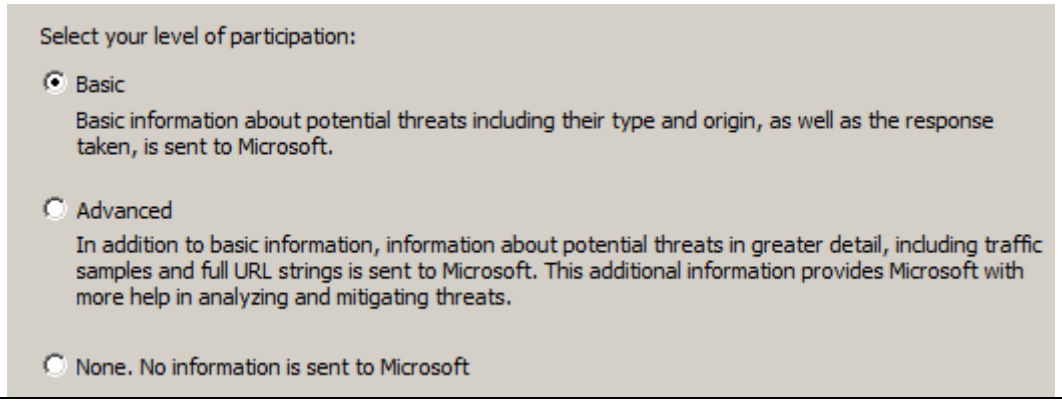
Bước 3: Click vào 1 Configure network settings → Chọn Edge firewall → Next→ Card INTERNET → Next→Finish


Getting Started - Network Setup Wizard
Internet Settings
Set the Internet settings based on information from your Internet Service Provider (ISP).
Network adapter connected to the Internet:
INTERNET

Bước 4: Configure network settings → Next→ I do not want to use the Microsoft Update services → Next → Yes


Use the Microsoft Update service to check for updates (recommended)
I do not want to use the Microsoft Update service
If the computer is not connected to the Internet, configuring the computer to use Microsoft Update may take several minutes.

Bước 5: No , I don't want to participate → Next → Chọn Basic → Next →Finish→Close


Select your level of participation:
Basic
Basic information about potential threats including their type and origin, as well as the response taken, is sent to Microsoft.
Advanced
In addition to basic information, information about potential threats in greater detail, including traffic samples and full URL strings is sent to Microsoft. This additional information provides Microsoft with more help in analyzing and mitigating threats.
None. No information is sent to Microsoft

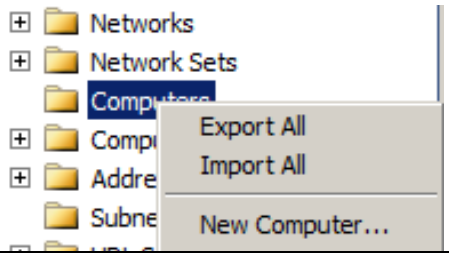
CẦU 2:

Tạo các tài khoản người dùng miền NV1, NV2, NV3 với mật khẩu đơn giản 12345 *(xem l ại QTM1***)**

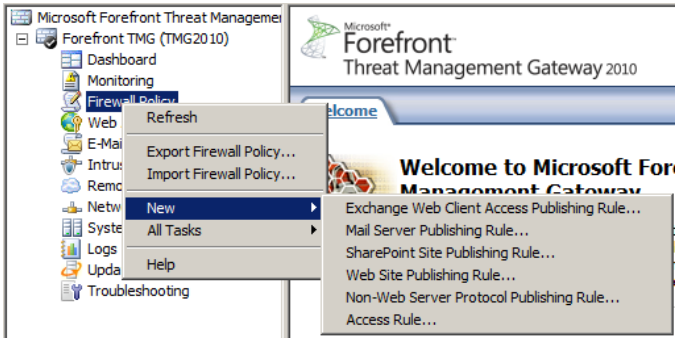
Cấu hình cho máy tính trong mạng ra được Internet thông qua máy TMG 2010 Server

Bước 1: Chọn phần Toolbox (TMG) → Click – Phải Computer → New

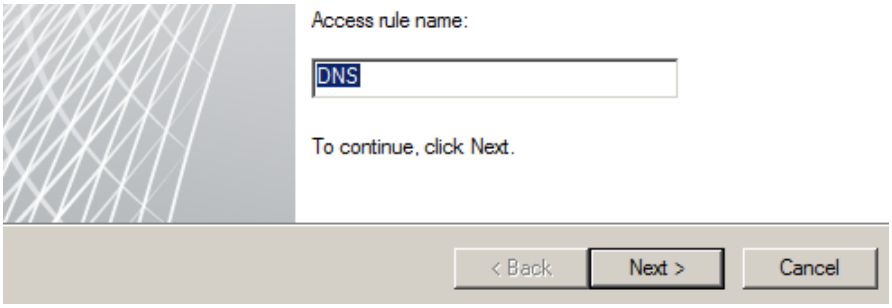
Computer…



Bước 2: Click – Phải Firewall Policy → New → Access Rule…

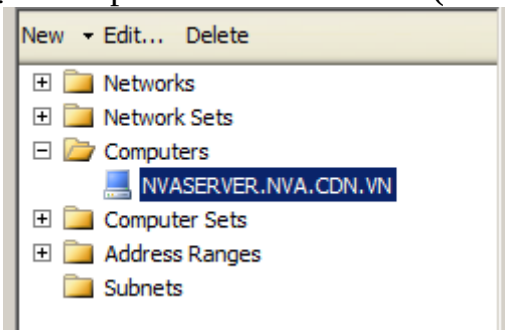


Bước 3: Tên Rule → Next



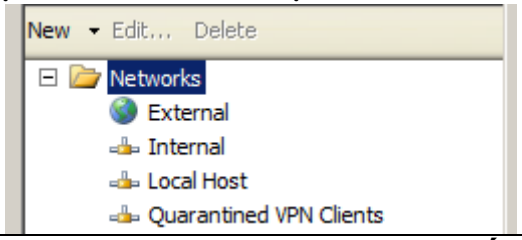
Chọn Add.. → Common Protocols → DNS → Close→Next→Next

Bước 4: Add… → Chọn Computer → Tên domain (NVA.CND.VN) → Close



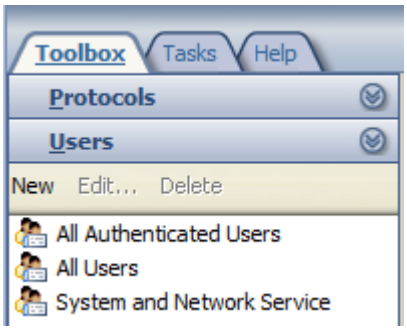
Next→Next

Bước 5: Add… → Chọn Networks → Chọn Local Host → Close→Finish



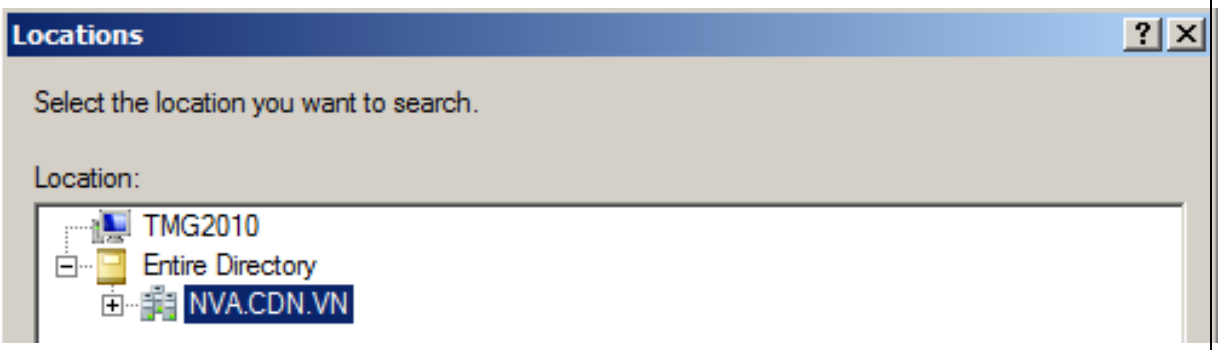
Tạo Rule cho phép tài khoản NV3 được phép truy cấp Internet không hạn chế

Bước 1: Toolbox → Users → New → Đặt tên (User NV3) → Next

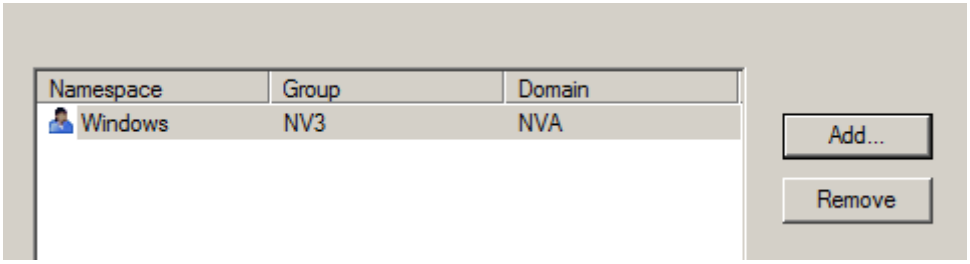


→Add… → Windows user and group…

Bước 2: Chọn (TMG2010) Locations… → Tích "+" Entire Directory → NVA.CDN.VN → OK



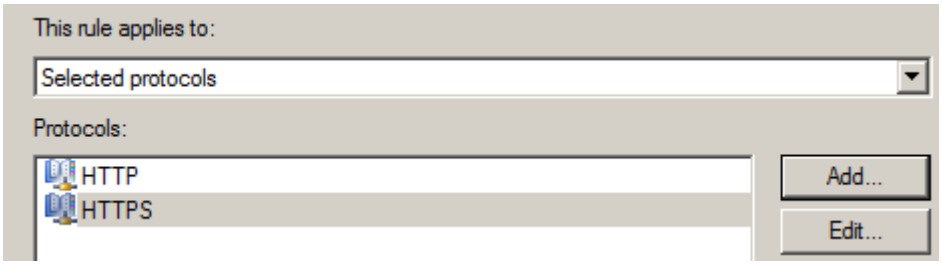
Bước 3: Next→ Next→Finish



Click → Apply → Apply → OK

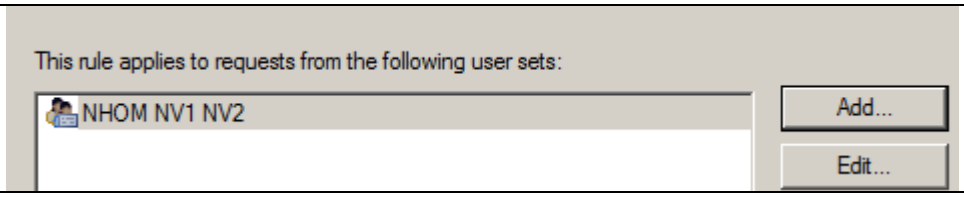
Tạo Rule cấm nhóm NV1, NV2 không được truy cập Internet trong giờ hành chính

Bước 1: Tên Rule → Next → Allow → Next→ Add… → Chọn Common Protocols → Add HTTP và HTTPS → Close

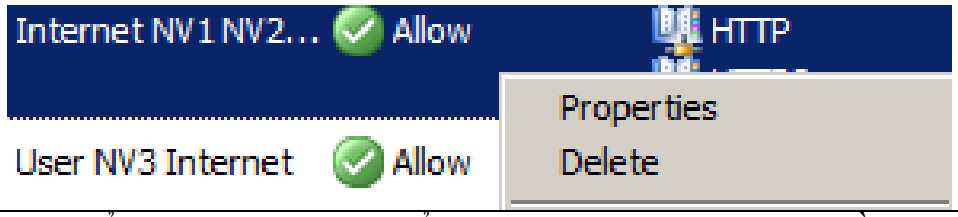


Add Internal và Local Host→Next

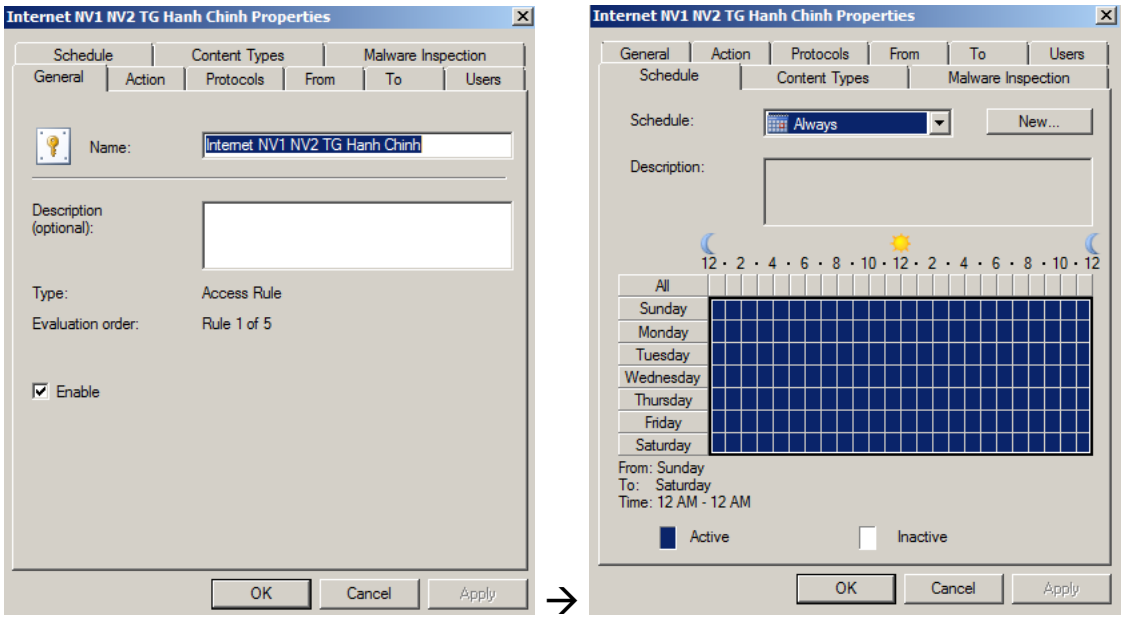
Bước 2: Add User NV3 → Next→Finish



Bước 3: Click – Phải Rule Truy cập internet của NV1 NV2 giờ hành chính → Properties

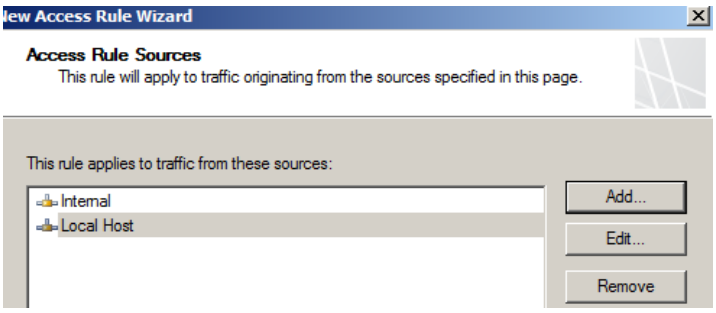


Bước 4: Cửa sổ Properties → Chuyển sang TAB Schedule → Phần Schedule → New….



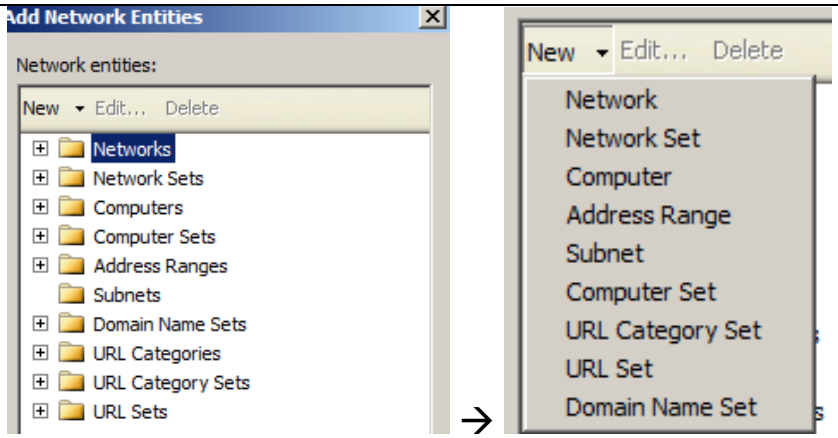
Thực hiện chuyển hướng trang Web http://nhatnghe.com về trang http://google.com.vn]

Bước 1: Tên Rule → Next → Deny → Next→ Add HTTP và HTTPS → Close

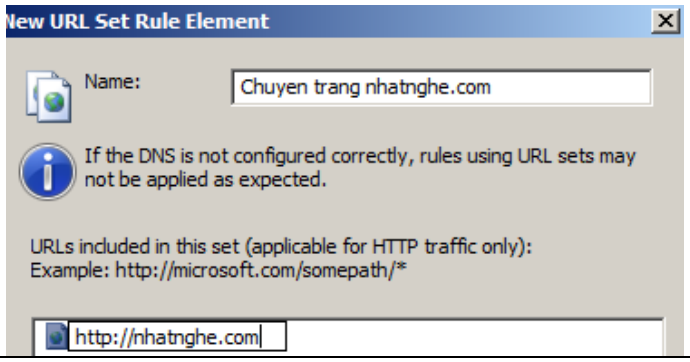


Add Internal và Local Host → Close

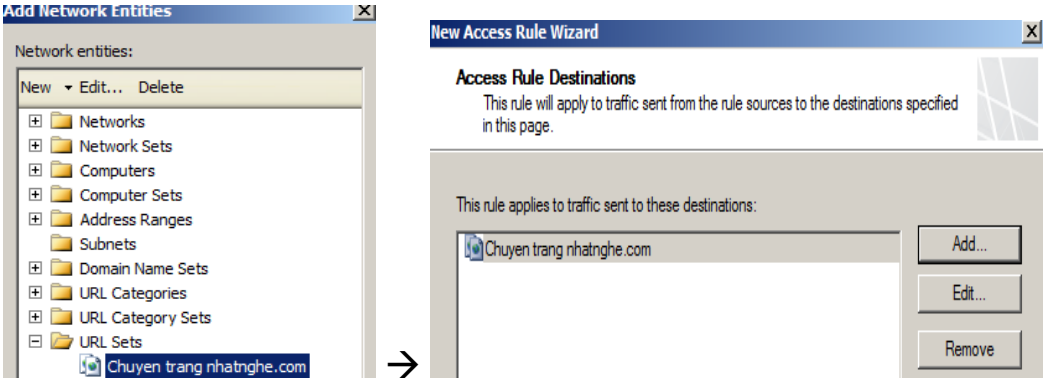
Bước 2: Cửa sổ Add Network Entities → New → URL Set



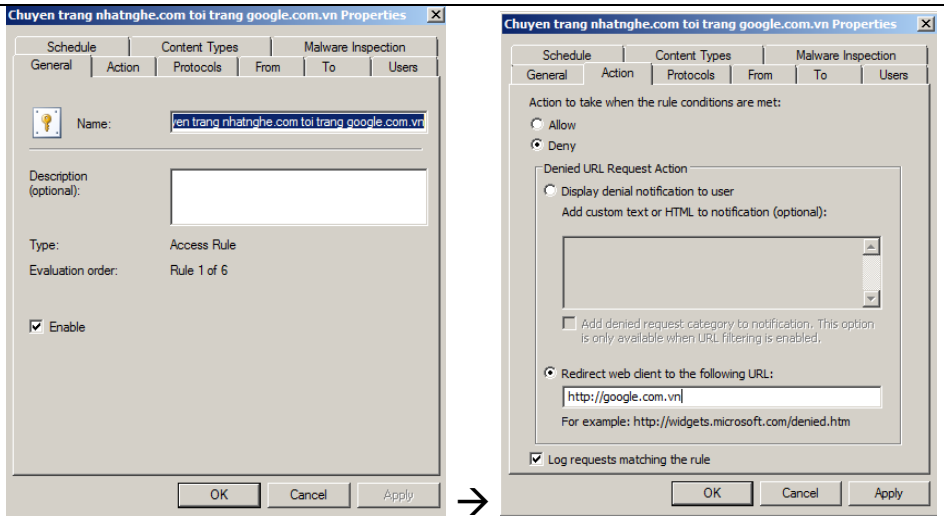
Bước 3: Name : Đặt tên → Add → ta sửa địa chỉ thành http://nhatnghe.com/* → OK


New URL Set Rule Element
Name:
Chuyen trang nhatnghe.com
If the DNS is not configured correctly, rules using URL sets may not be applied as expected.
URLs included in this set (applicable for HTTP traffic only):
Example: http://microsoft.com/somepath/*
http://nhatnghe.com

Bước 4: Tích "+" URL Sets → Chọn URL Set ta đã tạo ở trên → OK → Next→Finish



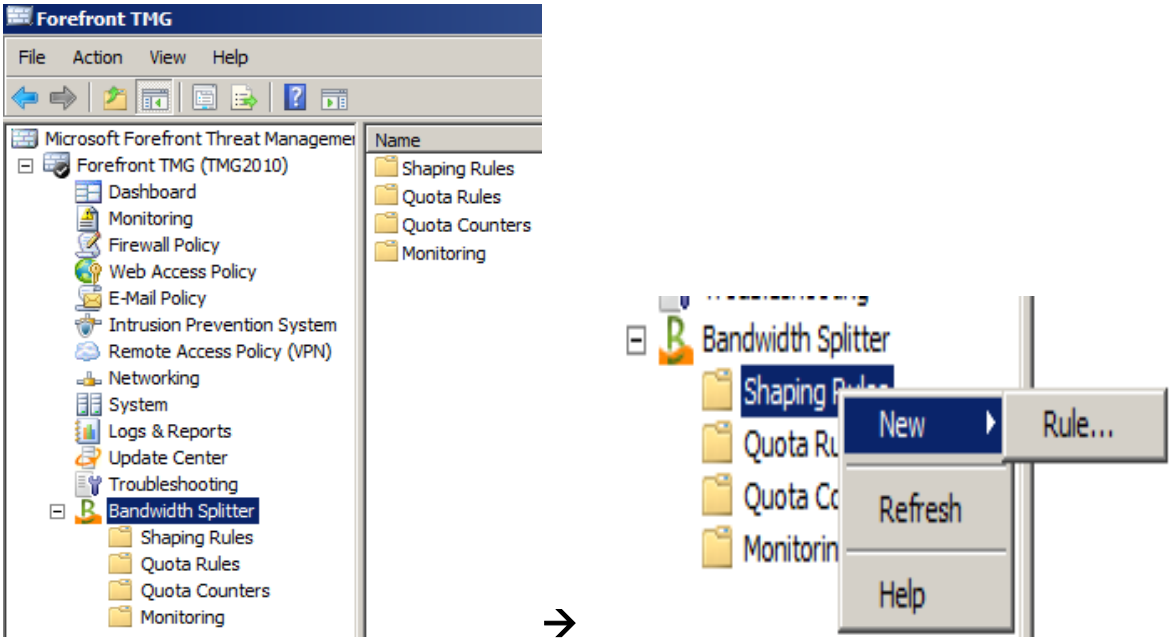
Bước 5: Ở cửa sổ Properties → TAB Action → Tích Deny → phần Denied URL Request Action ta tích vào Redirect web client to the following URL: gõ địa chỉ cần chuyển tới (http://google.com.vn) → Apply → OK



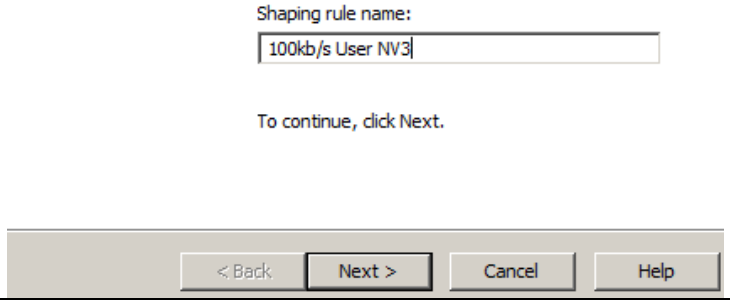
Click → Apply → Apply

Thực hiện ưu tiên băng thông cho NV3 gấp đôi băng thông các tài khoản còn lại

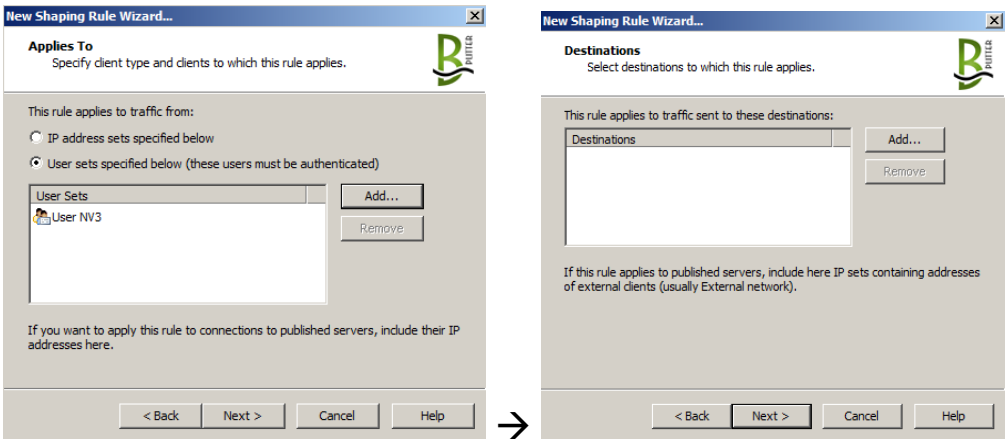
Bước 1: Click "+" Bandwidth Splitter → Click – Phải Shaping Rules → New → Rule



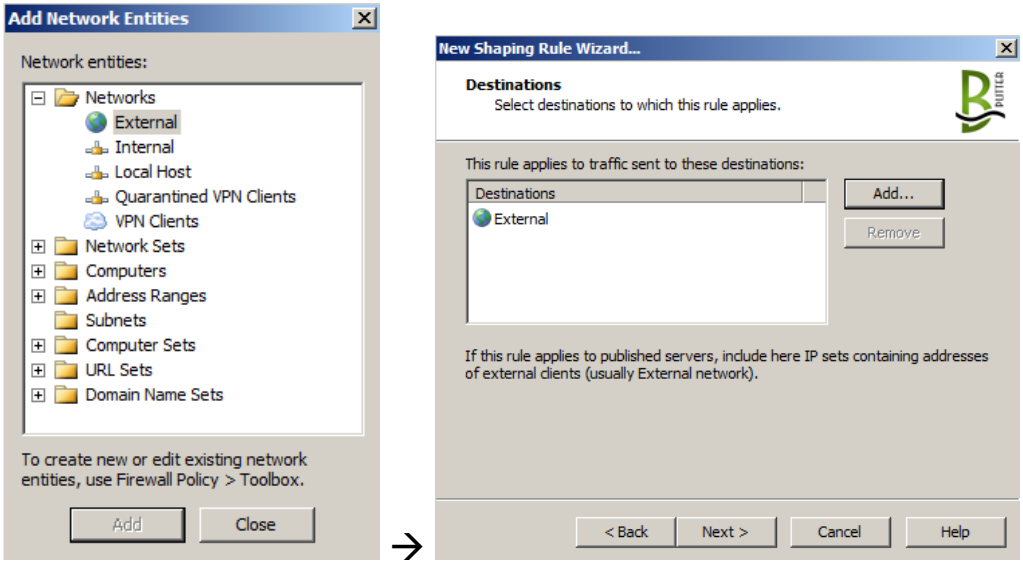
Bước 2: Đặt tên cho băng thông → Next→ Add… → User NV3 → Add → Close



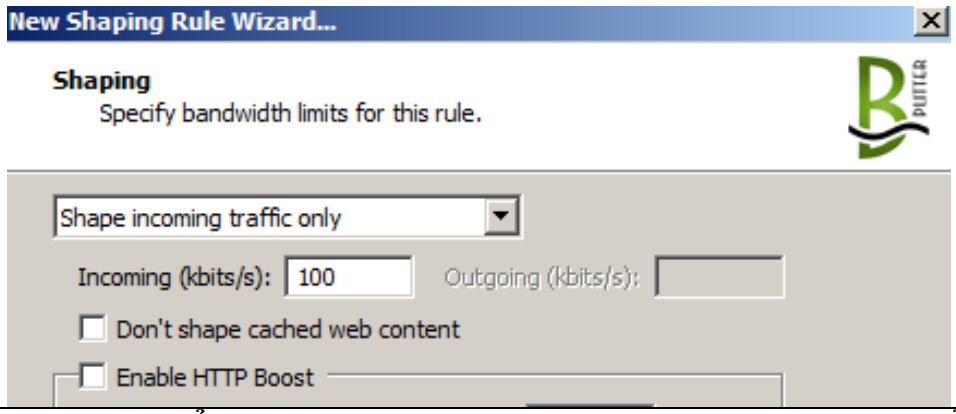
Bước 3: Next → Add…


New Shaping Rule Wizard...
Applies To
Specify client type and clients to which this rule applies.
This rule applies to traffic from:
IP address sets specified below
User sets specified below (these users must be authenticated)
User Sets
User NV3
Add...
Remove
If you want to apply this rule to connections to published servers, include their IP addresses here.
< Back
Next >
Cancel
Help
New Shaping Rule Wizard...
Destinations
Select destinations to which this rule applies.
This rule applies to traffic sent to these destinations:
Destinations
Add...
Remove
If this rule applies to published servers, include here IP sets containing addresses of external clients (usually External network).
< Back
Next >
Cancel
Help

Bước 4: Click "+" **Network** chọn **External → Add → Close → Next**

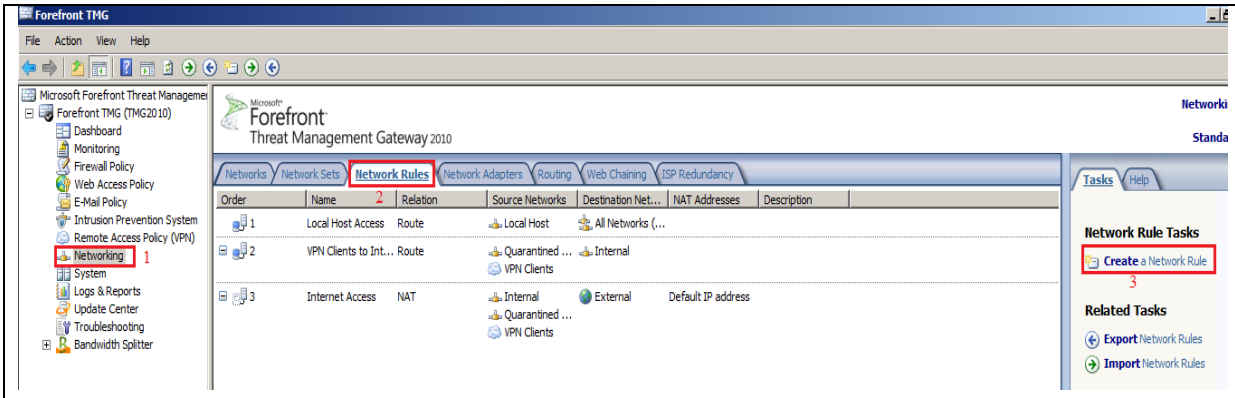


Bước 5: Chọn Shape incoming traffic only → Incoming (Kbits/s) : (VD : 100) → Next

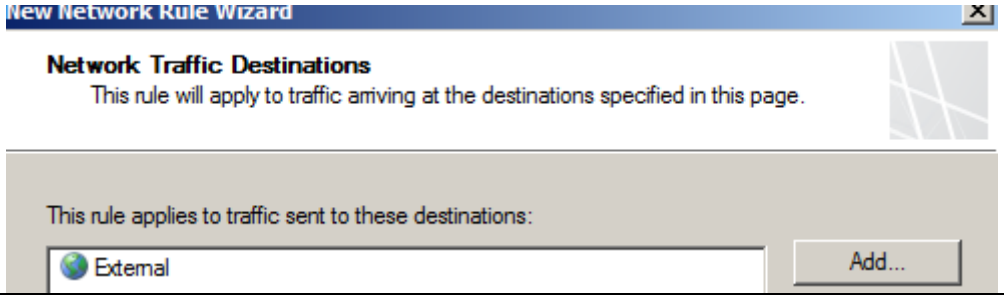


Publish Web, FTP để các người dùng trong mạng, ngoài mạng có thể truy cập được

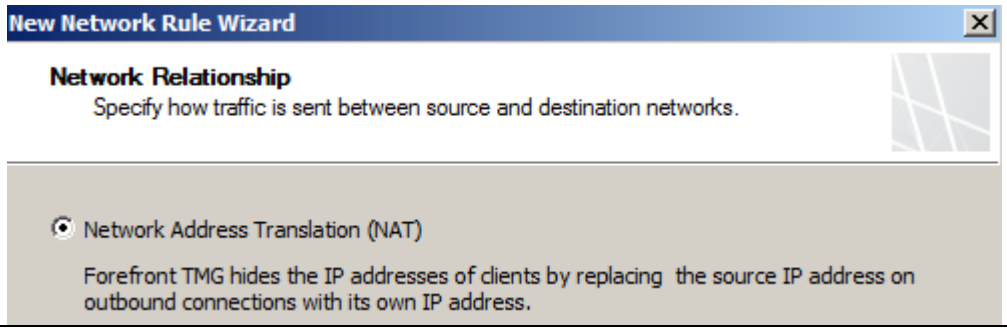
Bước 1: Networking → Network Rules → Create a Network Rules



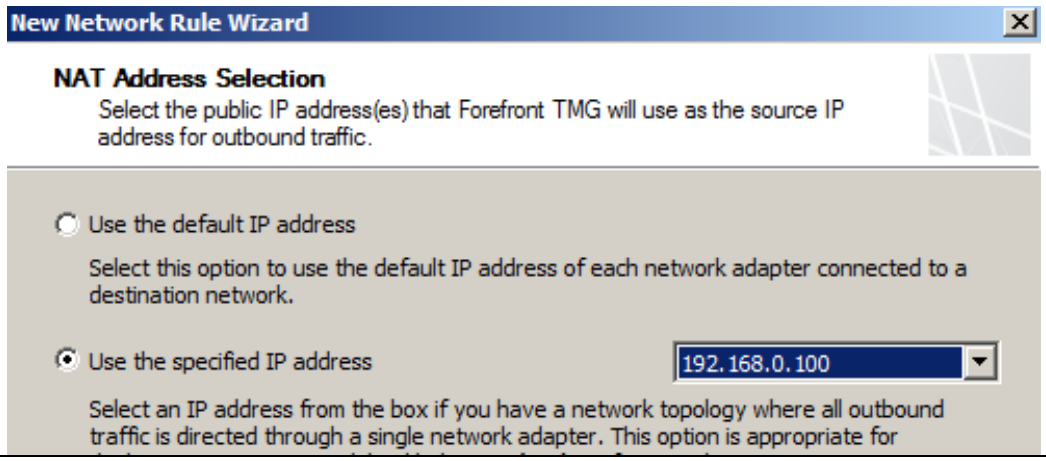
Bước 2: Name Rule → Next→ Add… → "+" Networks → Internal → Add → Close→Next


New Network Rule Wizard
Network Traffic Destinations
This rule will apply to traffic arriving at the destinations specified in this page.
This rule applies to traffic sent to these destinations:
External
Add...

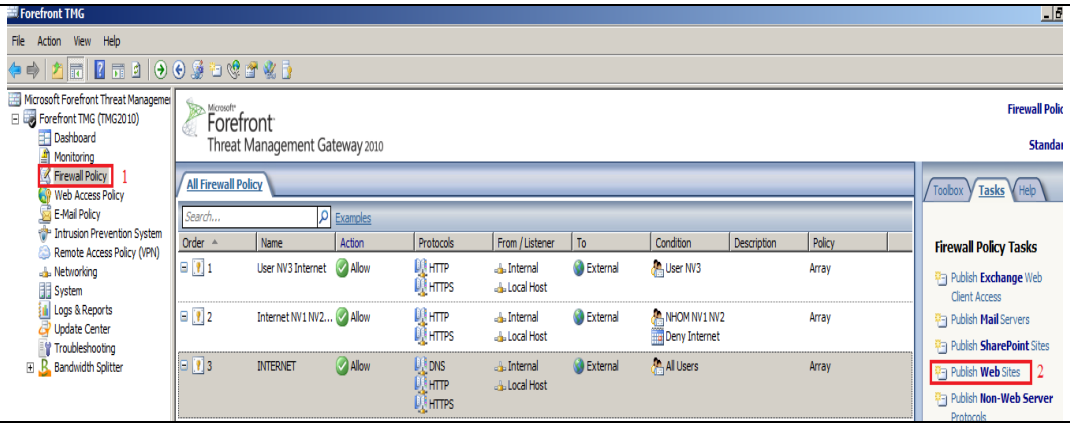
Bước 3: NAT → Next


New Network Rule Wizard
Network Relationship
Specify how traffic is sent between source and destination networks.
Network Address Translation (NAT)
Forefront TMG hides the IP addresses of clients by replacing the source IP address on outbound connections with its own IP address.

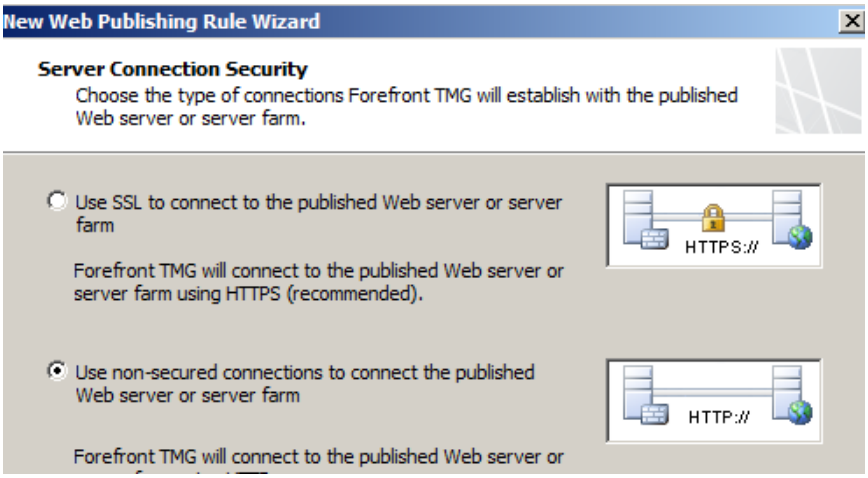
Bước 4: Use the specified IP address → Card Internet → Next→Finish


New Network Rule Wizard
NAT Address Selection
Select the public IP address(es) that Forefront TMG will use as the source IP address for outbound traffic.
Use the default IP address
Select this option to use the default IP address of each network adapter connected to a destination network.
Use the specified IP address
192.168.0.100
Select an IP address from the box if you have a network topology where all outbound traffic is directed through a single network adapter. This option is appropriate for

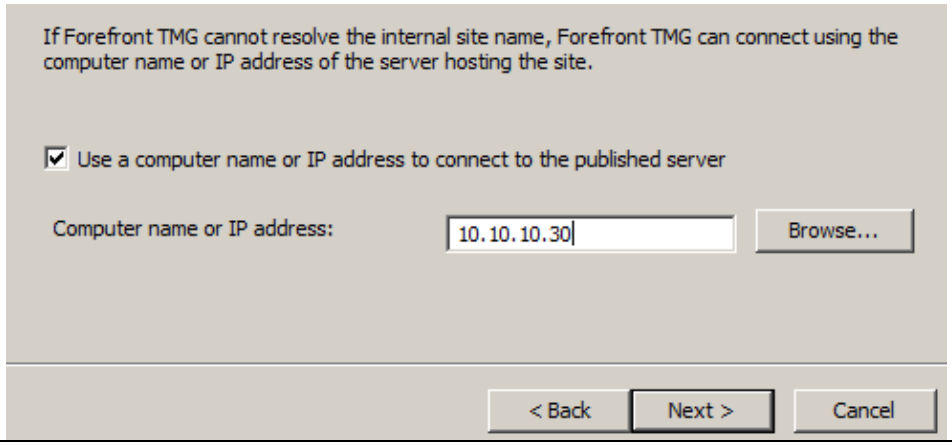
Bước 5: Firewall Policy → Publish Web Rules Sites



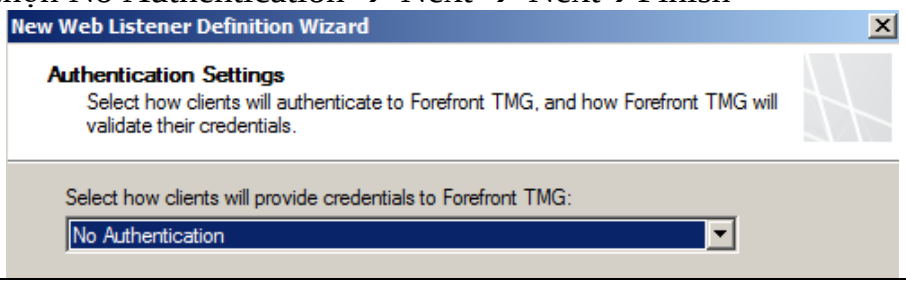
Bước 6: Name Rules → Next→Allow→Next→ Chọn HTTP:// → Next


New Web Publishing Rule Wizard
Server Connection Security
Choose the type of connections Forefront TMG will establish with the published Web server or server farm.
Use SSL to connect to the published Web server or server farm
Forefront TMG will connect to the published Web server or server farm using HTTPS (recommended).
HTTPS://
Use non-secured connections to connect the published Web server or server farm
Forefront TMG will connect to the published Web server or
HTTP://

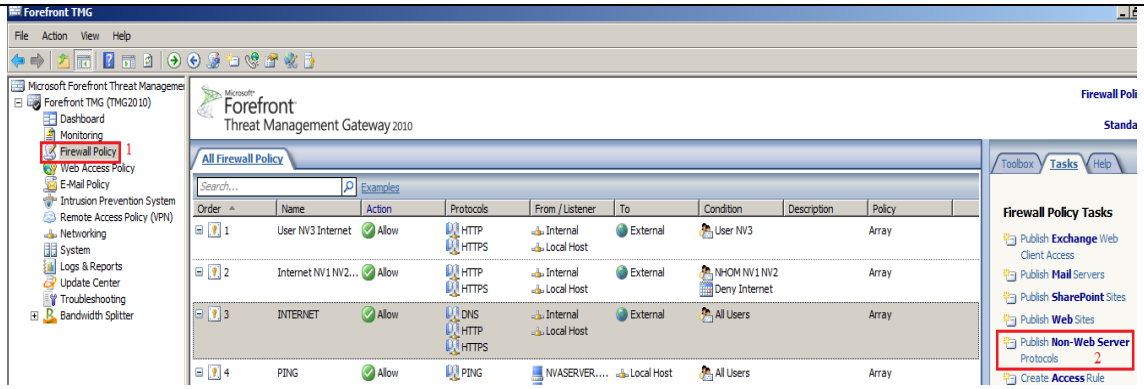
Bước 7: Internal site name (tên web) và tích vào Use a computer name or IP…. → Điền địa chỉ IP máy Web FTP


If Forefront TMG cannot resolve the internal site name, Forefront TMG can connect using the computer name or IP address of the server hosting the site.
Use a computer name or IP address to connect to the published server
Computer name or IP address:
10.10.10.30
Browse...
< Back
Next >
Cancel

Bước 8: Chọn No Authentication → Next → Next→Finish

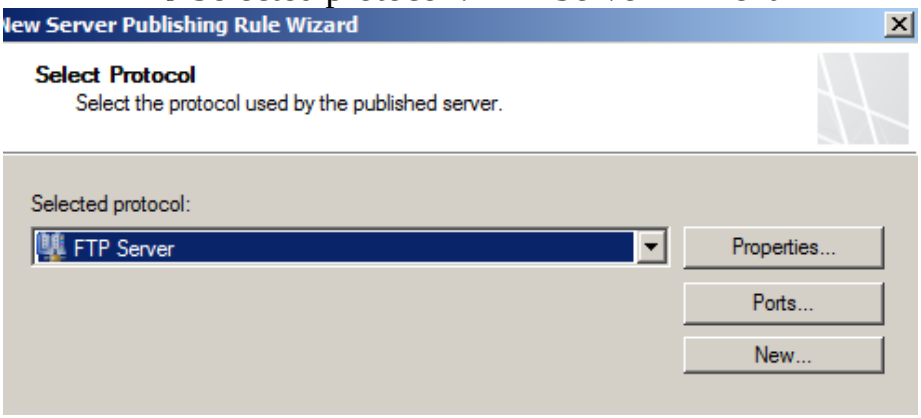

New Web Listener Definition Wizard
Authentication Settings
Select how clients will authenticate to Forefront TMG, and how Forefront TMG will validate their credentials.
Select how clients will provide credentials to Forefront TMG:
No Authentication

Bước 9: Firewall Policy → Publish Non-Web Server Protocols



Bước 10: Name Rule → Next → Địa chỉ máy Server Web – FTP → Next

→Selected protocol : FTP Server → Next



7.TÓM TẮT NỘI DUNG

- Cung cấp cơ chế truy xuất ủy quyền Web Site thông qua ISA firewall.
- Chuyển hướng theo đường dẫn truy xuất Web Site (Path redirection)
- Reverse Caching of published Web Site.
- Cho phép publish nhiều Web Site thông qua một địa chỉ IP
- Server-to-server communication: SMTP, NNTP: Cho phép Server Mail bên ngoài có thể giao tiếp với Server Mail nội bộ thông qua giao thức SMTP, NNTP

8.CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1:Nêu cách khắc phục Mail Mdaemon khi gửi có hiện tượng nhân đôi.
Câu 2:Trình bày cách xóa IP ra khỏi blacklist của Mail Mdaemon.
Câu 3: Client Access server role giao tiếp v ới internet client bằng những protocol nào ?
Câu 4: Để chặn thư điện từ một mail domain xác định, cần dù ng loại filter nào?

BÀI TẬP

Bài tập 1: Server Publishing thông qua ISA-2K6

Yêu cầu: Publishing 1webserver trong mạng nội ra ngoài internet để các client dù trong mạng nội bộ hay từ ngoài internet đều có thể truy cập. Thiết lập cơ chế điều khiển từ xa với Remote Desktop sao cho admin có thể điều khiển webserver từ một máy bất kỳ từ trong mạng nội bộ hoặc từ ngoài internet

Chuẩn bị

- 1 máy PC cài webserver
- 1 máy PC cài ISA 2006 kết nối internet
- Thiết lập địa chỉ IP cho mô hình và đấu nối mô hình mạng

Hướng dẫn làm bài

1. Xây dựng webserver, website defualt với internet infromation service (IIS)

B1: Mở Control Panel →Add Remove Programs → Add Remove Windows Components →Application Server →Nhấn Detail

B2: Đánh dấu chọn Internet Information Services (IIS) → Next

B3: Mở thư mục C:\Inetpub\wwwroot - Tạo một File Text Document có tên default.htm - Soạn thảo nội dung tùy ý cho File

2. Cấu hình cho phép truy cập Remote Desktop trên máy webserver

B1:Click phải My Computer → Properties

B2:Đánh dấn mục chọn Enable Remote Desktop in this computer → OK → OK

3. Cấu hình access rule và Publishing rule trên ISA cho webserver

B1:Tạo rule→đặt tên→cấp phép

B2:add các giao thức→finish

4. Cấu hình NAT inbound trên router ADSL

B1: Mở Internet Explorer → Nhập IP Router là 192.168.1.1 - Đăng nhập vào giao diện cấu hình Router ADSL (Username: admin, password: admin) →OK

B2: Chọn tab Advanced ◊ Nhấn nút Lan Clients - IP Address: Nhập IP máy ISA là **192.168.1.2 - Host Name: Nhập tên tùy ý → Add**

B3: Nhấn nút Virtual Server - Chọn Servers → Web Server →Add

B4: Chọn Apps → Win2k Terminal→ Add → Apply

5. Tạo Publis hostname bằng giao diện domain control panel của Yahoo

Bài tập 2: FTP Public Service

Yêu cầu: Cấu hình FTP Site mới→ FTP Publishing vào một website đang tồn tại

Chuẩn bị

- Sử dụng Windows Server 2008
- IIS 7.0 phải được cài đặt
- Đăng nhập với tài khoản quản trị
- Cài đặt, tải FTP Service http://www.iis.net/community
- Khởi động chương trình tải về bằng các chuột phải vào file vừ download và chọn Run as Administrator để cài đặt. Khi chương trình cài đặt bắt đầu, click Next.

Hướng dẫn làm bài

1.Cấu hình một FTP Site mới.

B1:Tạo một thư mục mới.

B2:Mở IIS Manager bằng các vào Start →Administrative Tool →Internet Information **Service** (IIS) Manager→ Trong IIS Manager, bên dưới Site**s**, bấm Add FTP Site.

2.Thêm FTP Publishing vào một website đang tồn tại.

B1:Mở "Sites**"** và tìm website mà bạn muốn thêm chức năng FTP vào, trong ví dụ này tên site là "Deffault Web Site"→Đánh dấu trang web **(**Deffault Web Site) và click chuột phải hoạc từ panel Action, chọn Add FTP Publishing

B2:Địa chỉ ip**:** Chọn địa chỉ ip cho site FTP mới của bạn, điều này có thể là "All Unassigned"

B3:Port: Cổng FTP mặc định là TCP port 21.

B4:Virtual Name: Bây giờ có thể sử dụng header cho site FTP, để trống, có nghĩa là nó sẽ đáp ứng những địa chỉ ip

B5:Chọn **"**Allow SSL" vì không có chứng chỉ SSL để bổ xung cho Site ftp.

3.Bảo mật một trang web FTP.

B1:Cấu hình một FTP site an toàn bằng commercial SSL→ vào Start → Administrative Tools → Internet Information Service (IIS) Manager→Trong IIS Manager, kích vào máy chủ FTP và đánh dấu các máy chủ và chọn Server Certificates

B2:Trong cửa sổ actions pane, chọn yêu cầu tạo giấy chứng nhận→ Chọn nhà cung cấp dịch vụ mật mã, để mặc định và kích Next→ chọn đường dẫn để lưu Certificate request và kick Finish

B3:Import Certificate Request→ Trong IIS Manager, kích vào máy chủ FTP và chọn Server Certificates→ Chọn Complete Certificate Request**…**

B4:Cấu hình một FTP site an toàn bằng self-signed SSL→Start →Administrative Tools → Internet Information Services (IIS) Manager →Trong IIS Manager, kích vào máy chủ FTP chọn Server Certificates →Trong Action pane, chọn Create Self-Signed Certificate→ Trang Specify Friendly Name, điền tên trang web FTP →OK→ Chọn chứng chỉ và các thiết lập cần thiết (Require SSL Connections) và nhấp Apply

Bài tập 3:Sử dụng ISA server 2006 hạn chế tấn công SQL INJECTION . Cài đặt, cấu hình như sau:

Yêu cầu:

- Xây dựng web site được thiết kế trên nền tảng công nghệ web .NET
- Dùng ISA Server 2006 để publish web site này.
- Khách hàng truy cập web site và attacker khai thác lỗi SQL Injection.
- Dùng ISA Server 2006 để lọc cách thức tấn công này.

Chuẩn bị

- 1 máy PC cài win2k3 →DC
- 1 máy PC cài win2k3→ISA
- 1 máy PC cài win7 dùng truy cập
- 1 sợi cáp bấm chéo
- 1 sợi bấm thẳng
- 1 router kết nối internet
- Phần mềm tạo trang web

Hướng dẫn làm bài

B1. Tạo trang web.

B2. Cấu hình Web Server

B3. Kiểm tra web site trong cục bộ.

B4. Publish web site

B5. Kiểm tra web site từ bên ngoài.

B6. Khai thác lỗi SQL Injection.

BÀI 10: MONITOR ISA SERVER
Mã bài:MĐ 32-09

Thời gian: 7 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

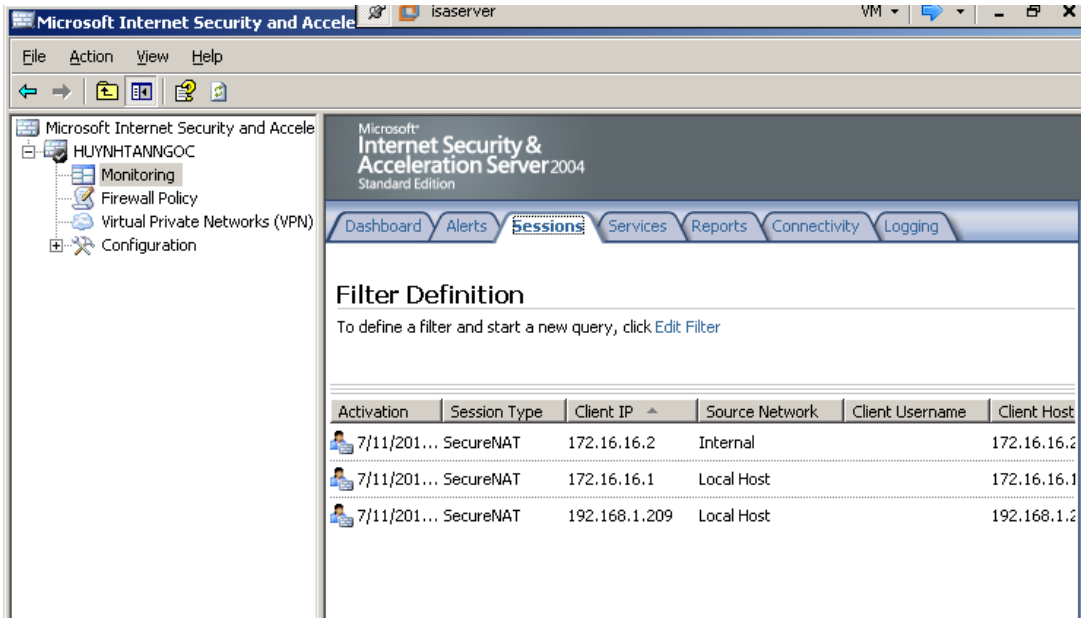
- Trình bày được các Tab trong Monitor;
- Phát hiện và khắc phục được các dịch vụ thông qua các tab trong Monitor;
- Thực hiện sao lưu và khôi phục lại máy ISA.
- Thực hiện các thao tác an toàn với máy tính

II.NỘI DUNG CHÍNH

1.Trình bày các tab trong Monitor

1.1 Tab Session:

Tab này trình bày cho ta biết đang có bao nhiêu Session diễn ra thông qua ISA và mỗi Session thông qua dạng nào như là SecureNAT, Web Proxy, Firewall Client để biết được các máy trong mạng nội bộ đang đi ra ngoài Internet thông qua ISA bằng dạng nào. Và ta thấy có địa chỉ IP là 172.16.16.2 đang ra ngoài Internet bằng dạng SecureNAT.


Microsoft Internet Security and Accele
isaserver
File Action View Help
Microsoft Internet Security and Accele
HUYNHTANNGOC
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Dashboard Alerts Sessions Services Reports Connectivity Logging
Filter Definition
To define a filter and start a new query, click Edit Filter
Activation Session Type Client IP Source Network Client Username Client Host
7/11/201... SecureNAT 172.16.16.2 Internal 172.16.16.2
7/11/201... SecureNAT 172.16.16.1 Local Host 172.16.16.1
7/11/201... SecureNAT 192.168.1.209 Local Host 192.168.1.2

Hình 10-1:màn hình Tab Session

1.2 Tab Services*:*

Tab này trình bày cho ta những dịch vụ nào của ISA đang chạy tốt và cũng thông qua tab này ta dùng để Restart từng dịch vụ khi mà ISA có trục trặc.

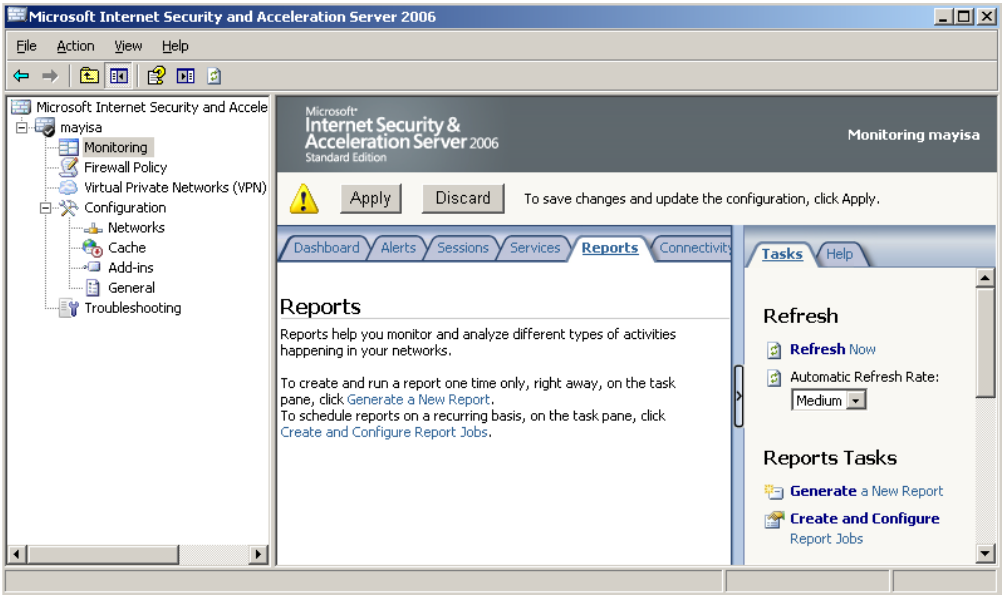
Ví dụ : khi ta áp1cái rule nào đó mà nó không chạy thay vì ta khởi động lại máy tính thì ta có thể Restart lại dịch vụ là Microsoft Firewall thôi. Bằng cách chọn Microsoft Firewall rồi click chuột phải chọn Stop khi nó stop

xong ta lại tiếp tục Restart lại.

Hình 10-2: màn hình Tab Services

1.3 Tab Report:

Tab này báo cáo thống kê giúp cho ta thống kê lại trong tháng đó ngày đó tuần đó máy nào trong mạng Lan đi ra web nhiều nhất chiếm nhiều băng thông nhất và lấy dung lượng nhiều nhất→double click vào Create and Configure Report Jobs.



Hình 10-3: màn hình Tab Report

1.4 Tab Connectivity:

Tạo ra các kết nối phục vụ choviệc kiểm tra.

Ví dụ: Có những trang web nào đó ở ngoài Internet mà nhu cầu ta rất thường xuyên truy cập thay vì trang web đó bị trục trặc gì đó ta phải ra ngoài CMD để ping kiểm tra coi thử nó có hoạt động không thì ta có thể xem trong Connectivity.

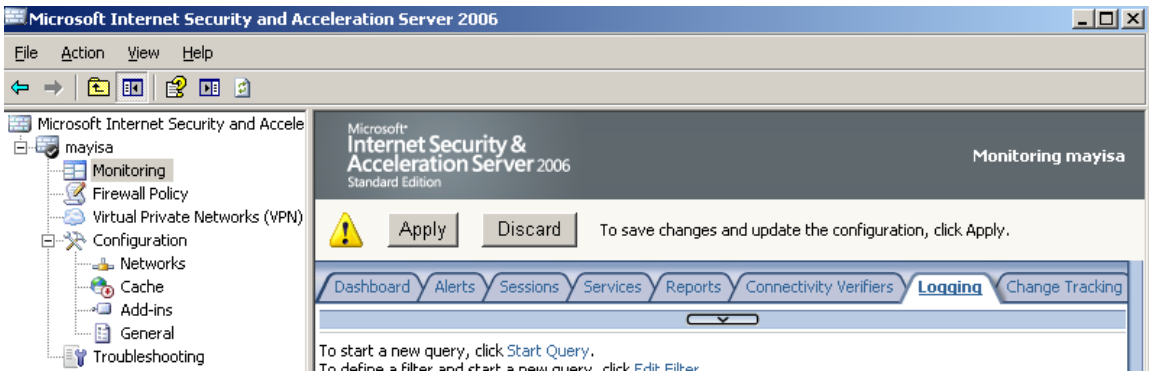
Mỗi lần ta muốn kiểm tra chỉ cần kích hoạt Connectivity và ta sẽ thấy nó báo là lỗi hay là không lỗi là ta biết→ Monitoring rồi chọn tab

Connectivity, double click →Create New Connectivity Verifier.

Hình 10-4:màn hình Tab Connectivity

1.5 Tab logging:

Đây là tab hay nhất trong Monitor cho ta biết rõ từng chi tiết IP nào đi đâu ra Internet và chiếm dung lượng bao nhiêu và đi ra bằng Rule nào và bị Rule nào chặn lại..v..v.Ta muốn coi IP nào truy cập web chiếm dung lượng bao nhiêu ta phải add thêm bytes Received→click phải chuột→Add→Remove để Add thêm Bytes Received.

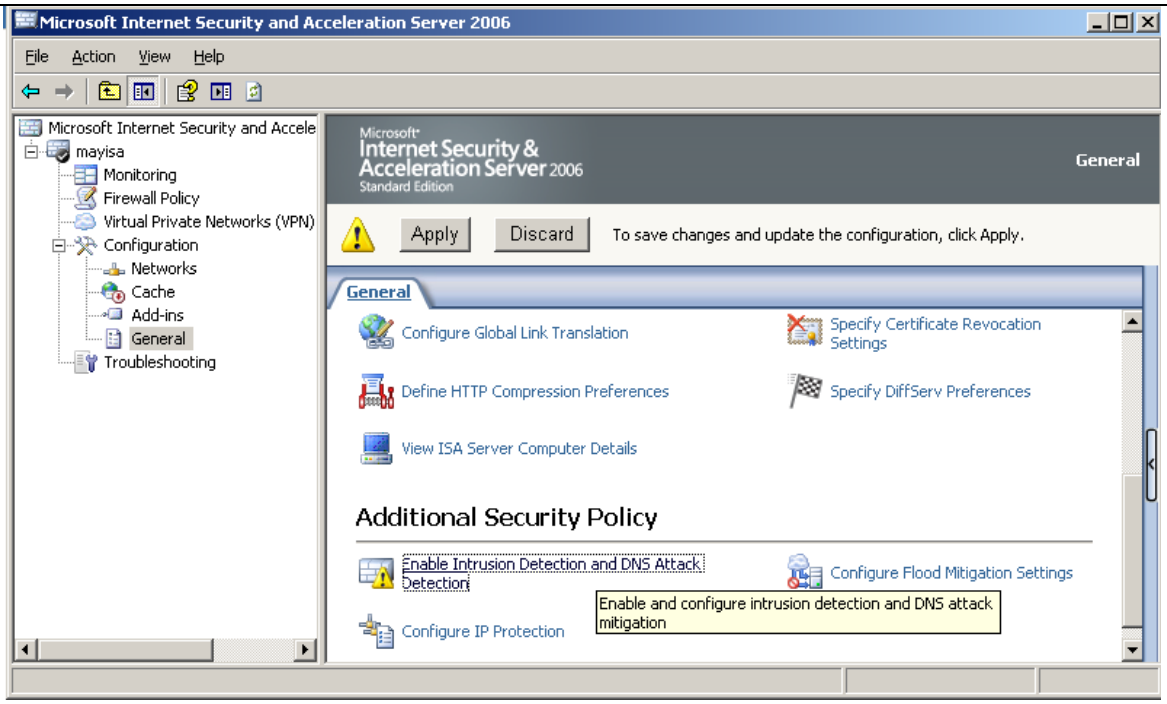


Hình 10-5:màn hình Tab logging

2.Phát hiện các đợt tấn công gửi mail cho admin

Cài đặt

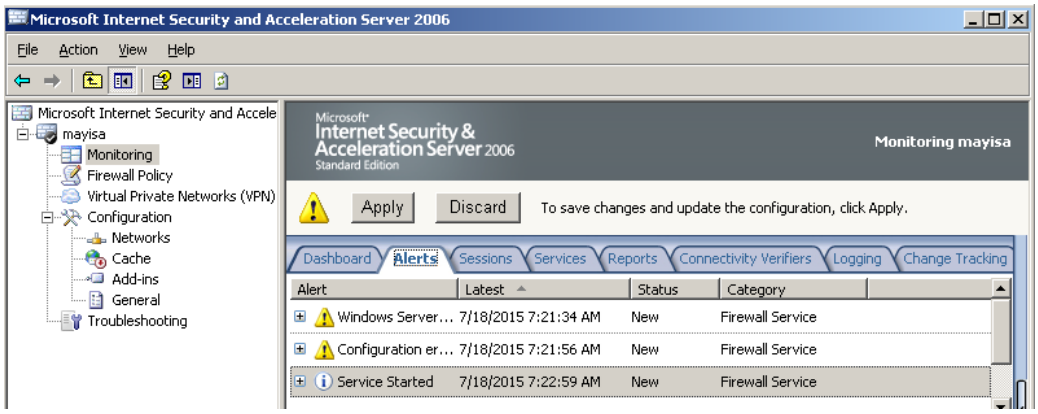
Bước 1: Mở ISA Server Management, chọn phần Configuration, chọn General, khung bên phải double click vào mục Enable Intrusion Detection and DNS Attack Detection.



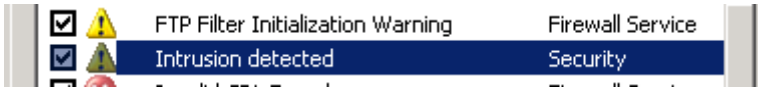
Bước 2: Hộp thoại Intrusion Detection, chọn Tab Common Attacks, đánh dấu chọn vào Port scan.

Bước 3: chọn Tab DNS Attack, đánh dấu chọn vào DNS zone transfer, chọn Ok

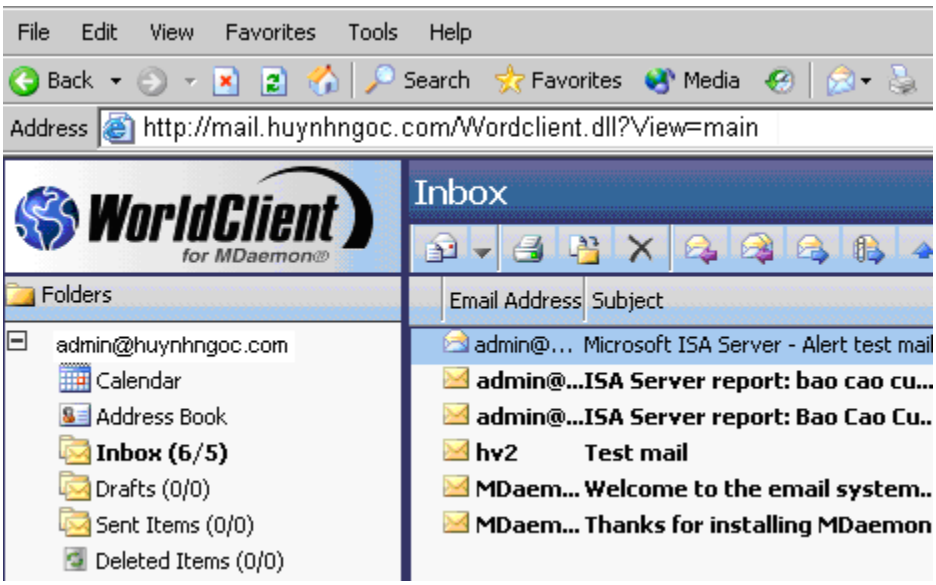
Bước 4: Tại TabMonitoring, chọn Tab Alerts, bên cửa sổ bên phải trong khung Tasks, chọn Configure Alerts Defintions



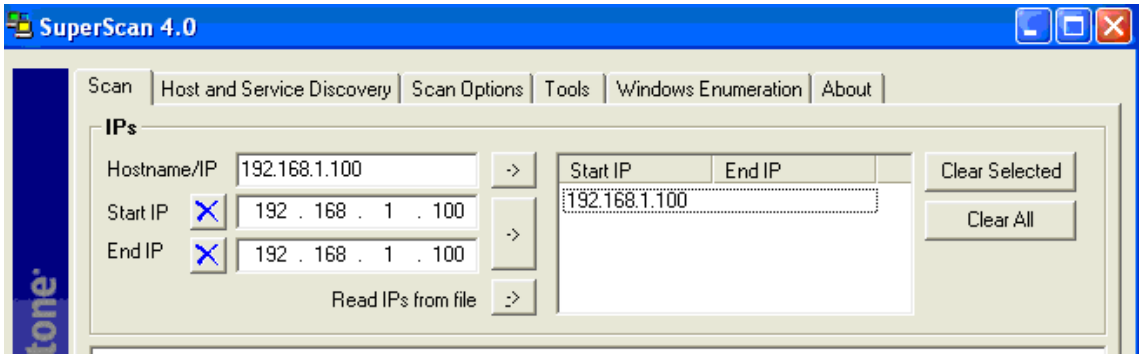
Bước 5: Hộp thoại Alerts Properties, chọn Intrusion detected rồi nhấn Edit.



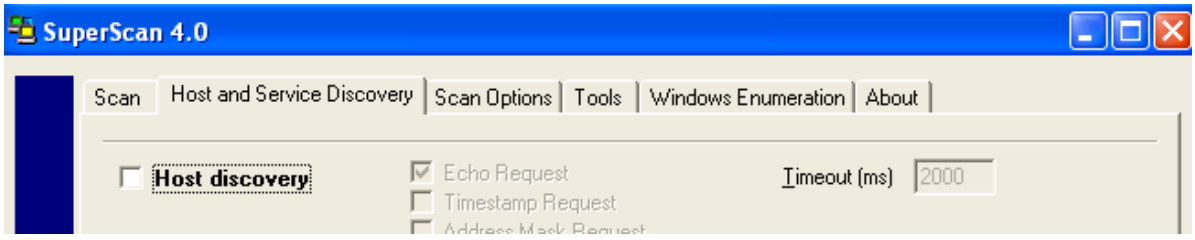
Bước 6: Sau khi cấu hình xong, mở Webmail lên Login với User Admin, kiểm tra trong mục Inbox và ta thấy có 1 Email cảnh báo do ta bấm nút Test khi cấu hình.



Bước 7: Lúc này tại máy Client, ta mở chương trình Scan Port lên để kiểm tra, trên trang. SuperScan4.0 nhập địa chỉ IP 192.168.1.100 trong khung StartIP và EndIP

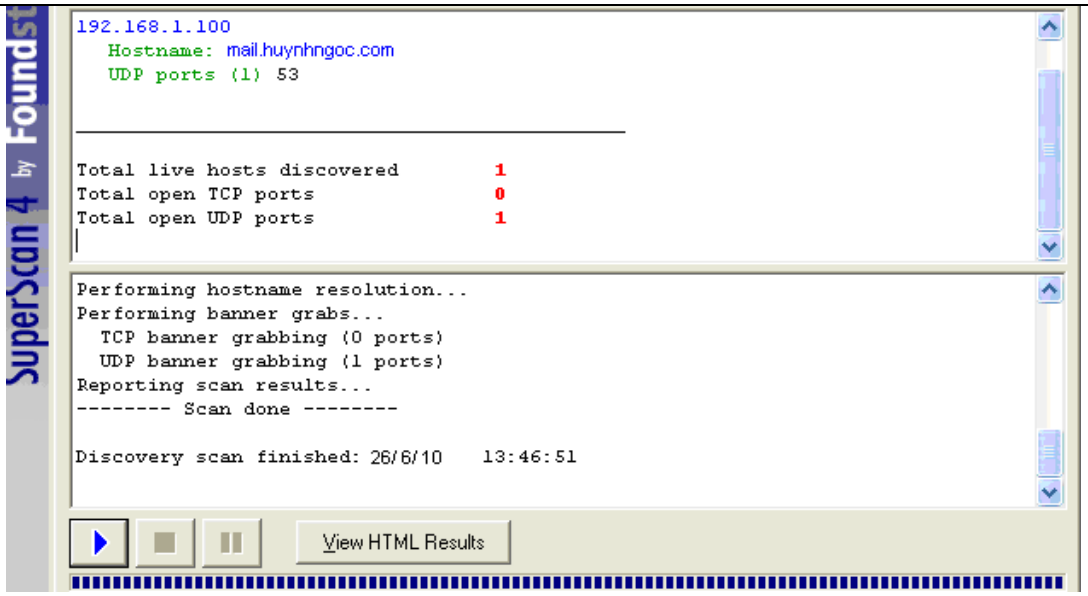


Bước 8: Chọn Tab Host and Service Discovery bỏ dấu check ô Host discovery

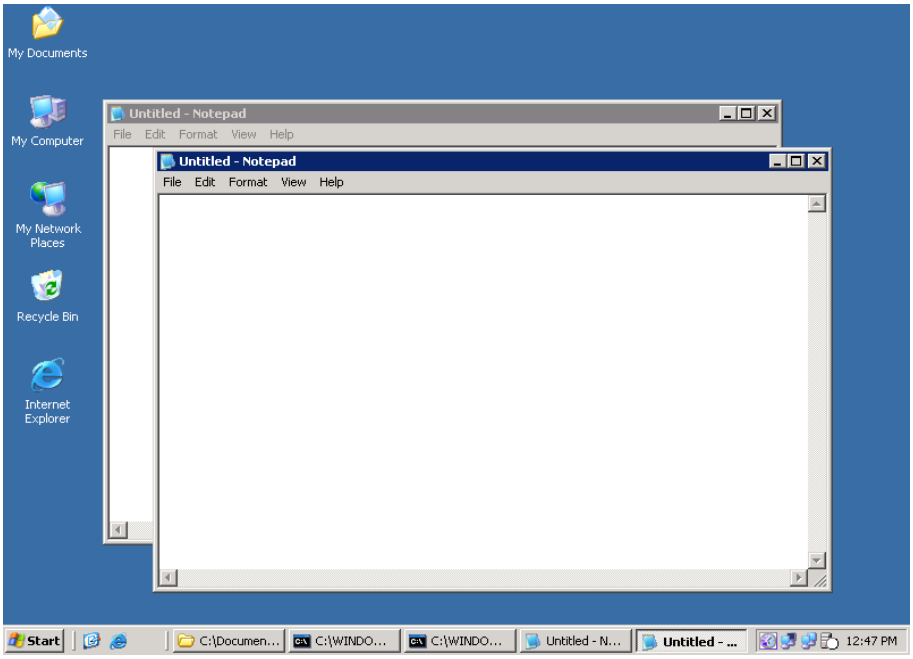


Bước 9: Và chọn tab Scan lại rồi bấm nút Play chương trình tự động Scanport

Chương trình Scan được 1Port muốn biết rõ port đó là gì ta bấm vàoView HTML Results.



Bước 10: trên máy ISA thì thấy Notepad được bật lên do có người đang tấn công Scanport.



Và mở WebMail lên đăng nhập vào User Admin thì thấy có IP 192.168.1.200 đang tiến hành Scanport

3.Network Templates

ISA Server 2006 Firewall mang đến cho chúng ta những thuận lợi to lớn, một trong những số đó là các Network Temlates. Với sự hỗ trợ các Templates mà chúng ta có thể cấu hình tự động các thông số Network, Network Rule và Access Rules. NetworkTemplates được thiết kế nhanh chóng tạo được cấu hình nền tảng cho những gì mà chúng ta có thể xây dựng các loại Network Templates:

Các loại Network Templates:

Edge Firewall: được sử dụng khi ISA gắn 2 card Network. Có một Network

interface kết nối đến Internet và một Network interface kết nối với Internal

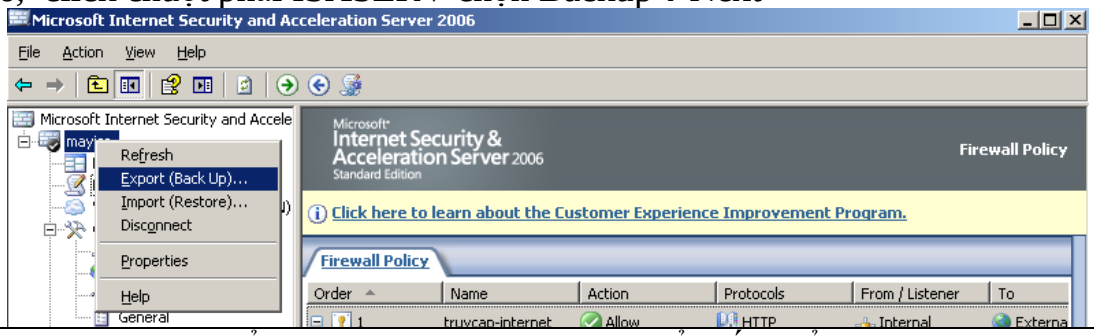
Network.3-Leg Perimeter: được sử dụng khi Firewall gắn 3 Card Network. Có Network interface (kết nối Internet) và Internal interface (kết nối mạng nội bộ) và DMZ interface (kết nối mạng vành đai – Perimeter Network).

Front Firewall : Đóng vai trò một frontend firewall trong mô hình back-to-back Back-to back là mô hình kết nối 2 Firewall làm việc với nhau theo kiểu trước (front) sau (back) phía ngoài Front Firewall là Internet giữa Front và back Firewall có thể là DMZ network và phía sau back Firewall là Internal network.Single Network Adapter: được áp dụng khi ta muốn loại chức năng Firewall đi. Được dùng trong những trường hợp khi ISA chỉ có 1 card Network đóng vai trò là hệ thống lưu giữ cache – Web caching server.

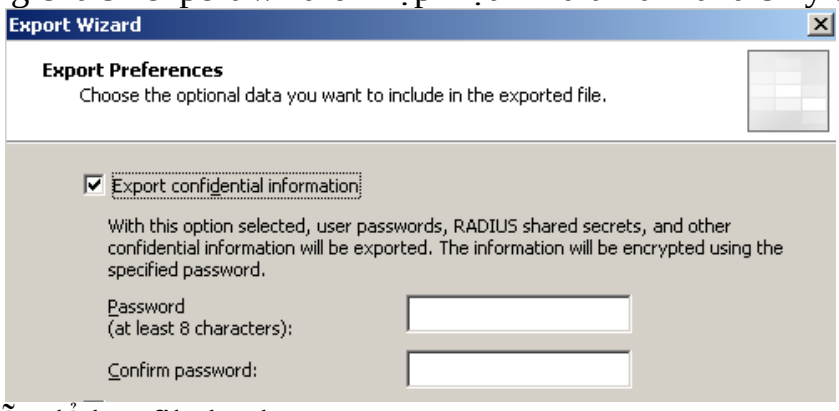
4.Backup và Restore

4.1 Backup

Bước 1: Trong cửa sổ Mircrosoft Internet Security and Acceleration Server 2006, click chuột phải ISASERV chọn Backup→Next



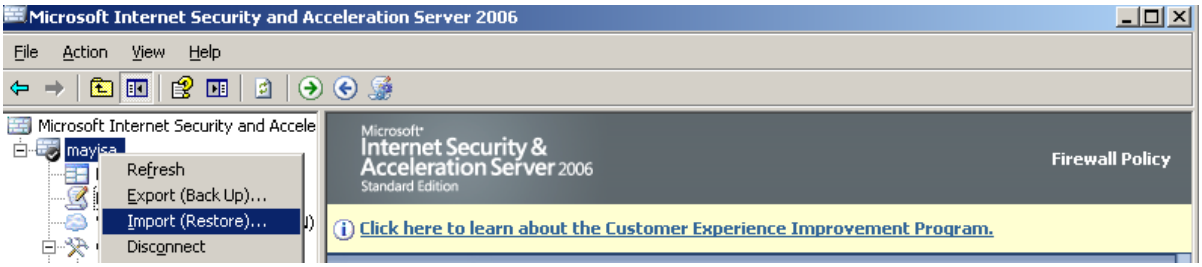
Bước 2: Trong cửa sổ export wizard nhập mật khẩu tối thiểu là 8 ký tự→next


Export Wizard
Export Preferences
Choose the optional data you want to include in the exported file.
Export confidential information
With this option selected, user passwords, RADIUS shared secrets, and other confidential information will be exported. The information will be encrypted using the specified password.
Password (at least 8 characters):
Confirm password:

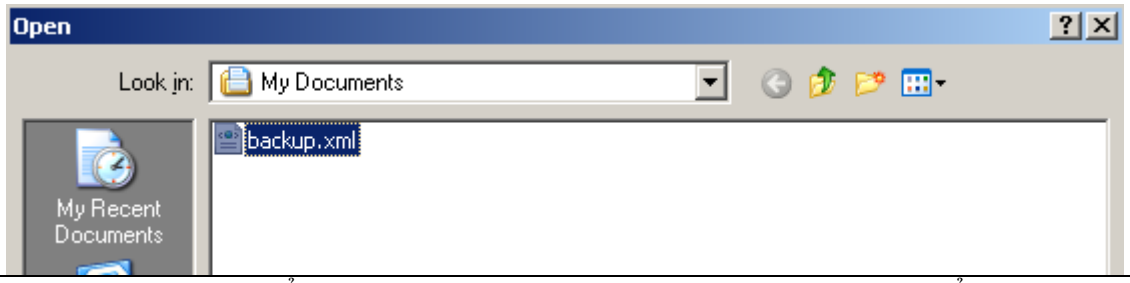
Chỉ đường dẫn để lưu file backup

4.2 Restore

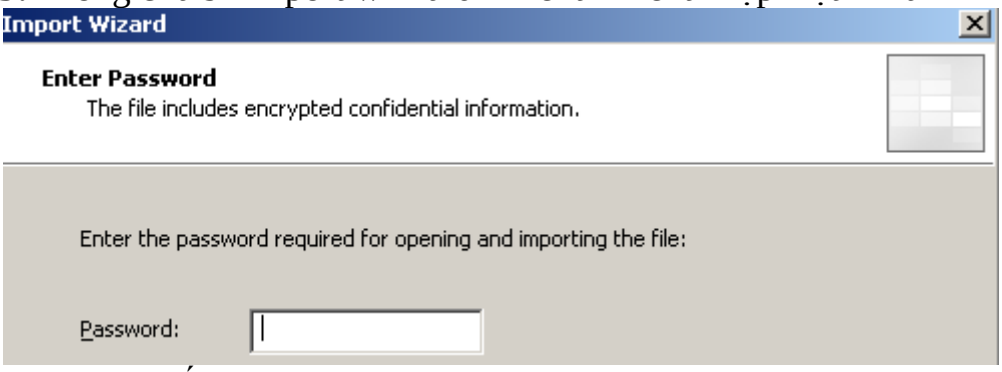
Bước 1: Trong cửa sổ Mircrosoft Internet Security and Acceleration Server 2006, click chuột phải ISASERV chọn Restore→Next



Bước 2:Tìm đường dẫn chứa file backup→ Mở file backup



Bước 3: Trong cửa sổ import winzard→Next→Next nhập mật khẩu →Next


Import Wizard
Enter Password
The file includes encrypted confidential information.
Enter the password required for opening and importing the file:
Password:

Nhấn finish hoàn tất quá trình Restore

Bài tập: Chuyển đổi từ ISA 2006 sang TMG 2010.

Yêu cầu: Backup config trên ISA Server 2006→ Restore config trên Forefront TMG 2010

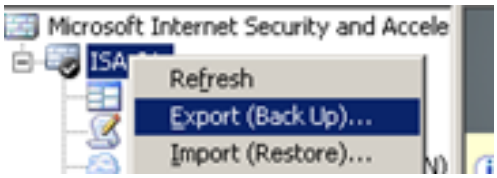
Chuẩn bị:

- 1 máy PC cài win2k3 →ISA 2006 tạo các rule
- 1 máy PC cài win2k8→ TMG 2010

Thực hiện

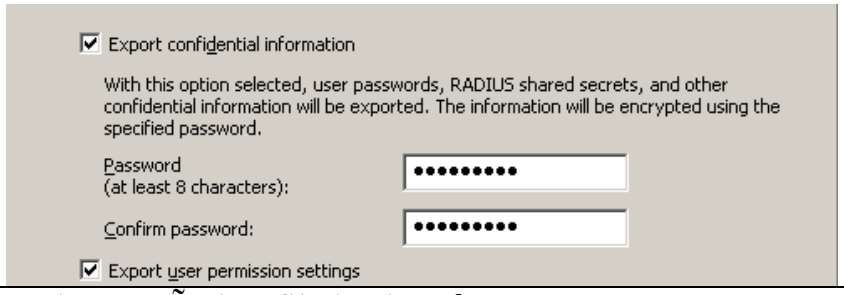
1. Backup config trên ISA Server 2006

Bước 1: Truy cập vào cửa sổ quản lý của ISA Server, trên ISA Server click chuột phải chọn Export (Back Up)

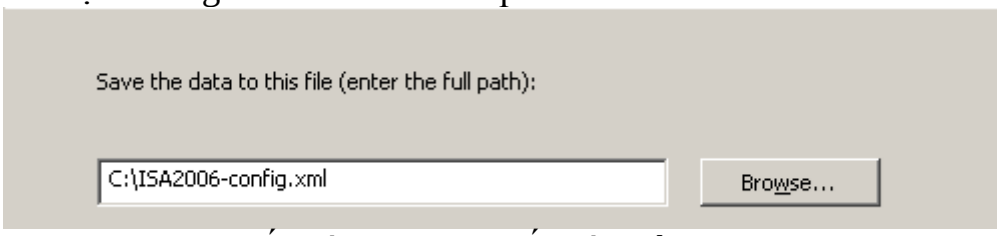


Cửa sổ Export Wizard → Next.

Bước 2: Trong khung Export Preferences :→Đánh dấu check vào Export confidential infomation và nhập mật khẩu bảo vệ file backup→Đánh dấu check vào Export user permission settings


Export confidential information
With this option selected, user passwords, RADIUS shared secrets, and other confidential information will be exported. The information will be encrypted using the specified password.
Password (at least 8 characters):
Confirm password:
Export user permission settings

Bước 3: Chọn đường dẫn lưu file backup→Next

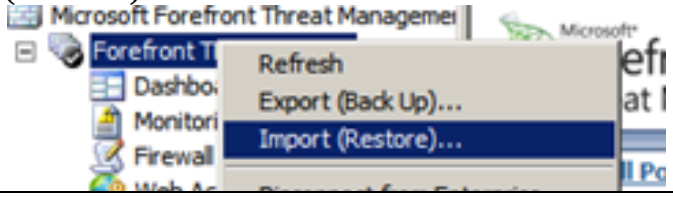


Tiến trình backup tiến hành→Finish

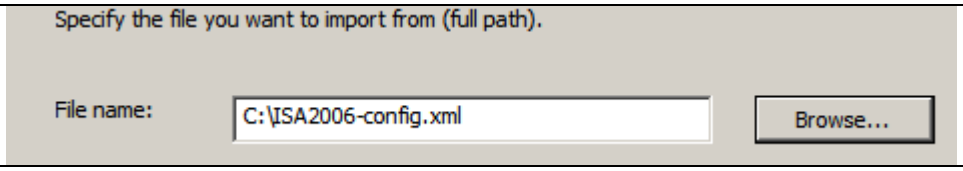
Bước 4: Chép file backup ra USB hoặc một phân vùng khác, Formart phân vùng chứa hệ điều hành Windows Server 2003 và tiến hành cài đặt Windows Server 2008 x64 (khuyến khích sử dụng Windows Server 2008 R2). Sau khi cài đặt xong Windows và đặt 02 IP card mạng giống như cũ thì ta tiếp tục cài đặt Forefront Threat Management Gateway (TMG) 2010.

2.Restore config trên Forefront TMG 2010

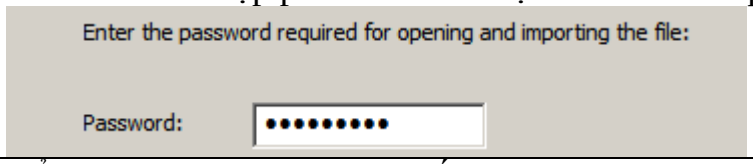
Bước 1: Truy cập cửa sổ quản lý Forefront TMG, trên Forefront TMG click phải chọn Import (Restore)



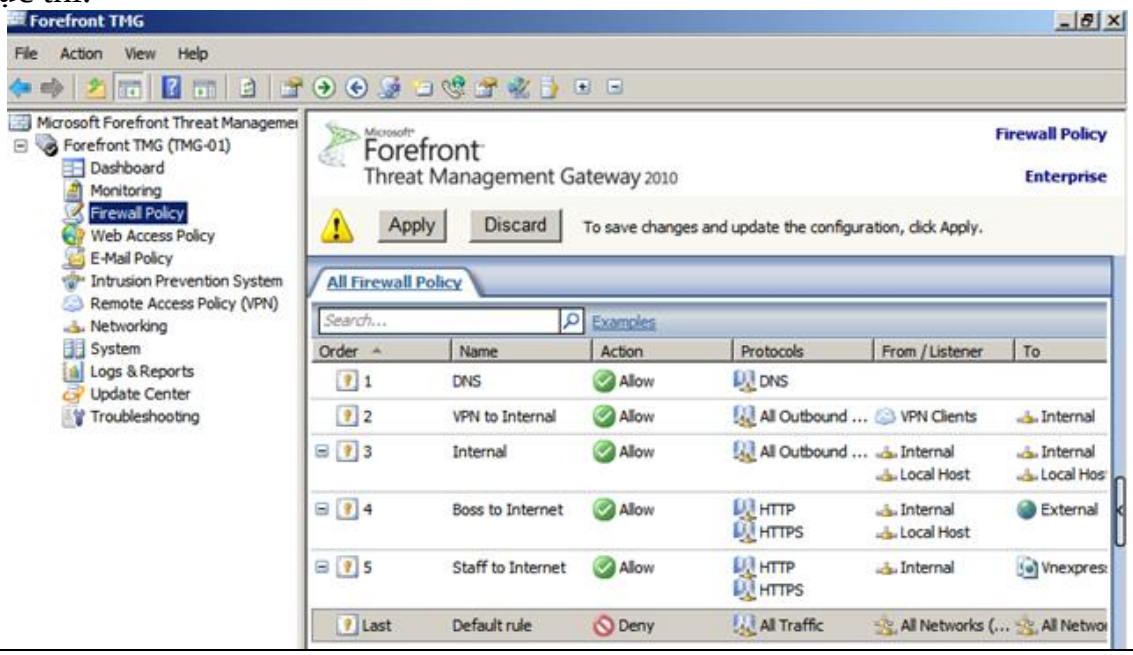
Bước 2: Cửa sổ Import Wizzard →Next→ file backup của ISA Server 2006→ Next



Bước 3: Forefront TMG cảnh báo là file backup config ta đang sử dụng của một phiên bản cũ → OK→ Nhập password bảo vệ của file backup.



Bước 4: Nhấn kiểm tra các Rules và các thiết lập đã được restore→ Apply để thực thi.



5- TÓM TẮT NỘI DUNG

- Cung cấp nhiều công cụ hữu ích cho việc quản trị hệ thống cũng như đảm bảo an toàn cho hệ thống thư điện tử.
- Cho phép chống Spam và không cho phép gửi và nhận thư đến hoặc từ một địa chỉ xác định.
- Quét các thư đi qua để tìm và diệt virus email.
- Tạo các nhóm người dùng
- Tạo thư mục cho phép mọi người được quyền sử dụng chung dữ liệu ở trong thư mục.
- Cho phép người dùng có thể quản lý hộp thư của mình sử dụng Web Brower.
- Cho phép quản trị hệ thống thư điện tử từ xa và Web Admin cho phép quản trị trên Web Brower vv...

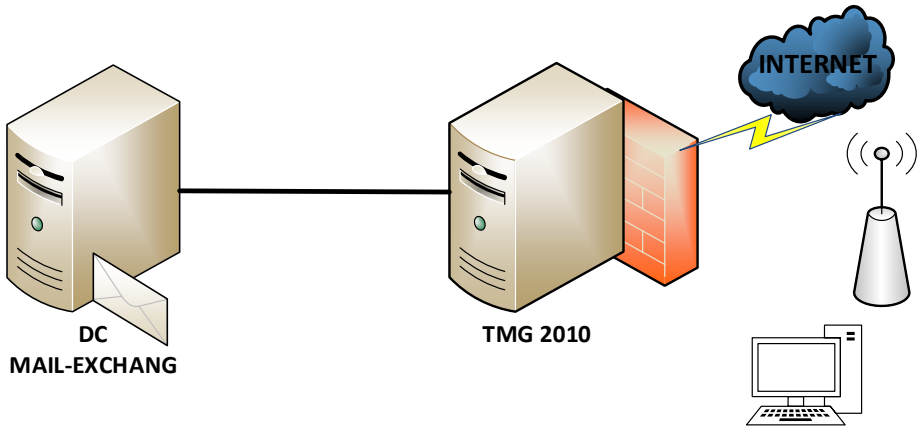
6- CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày ý nghĩa. Cấu hình Web Proxy Client, cấu hình Firewall Client.
Câu 2: Trình bày khái niệm về mailserver, nêu trình tự gửi và nhận mail trên ISA

BÀI TẬP

Bài tập 1: Kết hợp Exchange 2010 và TMG 2010



Yêu cầu: Cài đặt Exchange Server. Tạo Mailbox User & kiểm tra gởi nhận E-mail
Trên TMG 2010
Chuẩn bị

- 1 máy PC cài win2k8→DC→ cài Exchang 2010
- 1 máy PC cài win2k8→ TMG 2010
- 1 máy PC truy cập Internet→nhập và gửi mail
- 1 sợi cáp bấm chéo
- 1 sợi cáp bấm thẳng
- Thiết lập IP tùy theo yêu cầu

Hướng dẫn làm bài

1.Cài đặt Exchange Server. (xem lại đề số 3 trong bộ đề thi tốt nghiệp đã hướng dẫn)
2.Tạo Mailbox User & kiểm tra gởi nhận E-mail. **.** (xem lại đề số 3 trong bộ đề thi tốt nghiệp đã hướng dẫn)
3.Kết hợp Exchange 2010 và TMG 2010

B1*:* **Kích hoạt sự bảo vệ email→ E-Mail Policy→ Kích vào nút E-Mail Policy**

B2: kích liên kết Configure E-Mail Policy→ Welcome to the E-Mail Policy Wizard→ Next.

B3: Add →Internal mail servers→ Computer→Nhập vào tên của máy chủ SMTP và địa chỉ IP của máy chủ→ OK.

B4: Next → Internal Mail Server Configuration→ Select Addresses → địa chỉ IP nào đó để chấp nhận mail gửi đi từ máy chủ SMTP bên trong→Next

B5: External E-Mail Listener Configuration→ External → Select Addresses → một địa chỉ IP nào đó là địa chỉ mà bạn muốn chấp nhận mail gửi đi.

B6: Trong hộp FQDN or IP address→ Fully Qualified Domain Name → TMG firewall → SMTP session, →DNS ngược cho name này phân giải địa chỉ IP chính xác, đó là địa chỉ đang nhận mail gửi đến→ Next.

B7: Microsoft Forefront Threat Management Gateway→System Policy Rules → SMTP → Yes→ Apply

4.Cấu hình chính sách email

B1: External_Mail_Servers→ E-Mail Policy→OK

B2: File Filtering → File Filtering→ File Filters→ Add→ File Types.

B3: File Names→ Remediation→ Options→ Message Body Filters→OK

Bài tập 2: Backup và khôi phục toàn bộ cấu hình trên TMG 2010

Yêu cầu: Cấu hình export và import toàn bộ cấu hình Forefront TMG 2010

Chuẩn bị: Khởi chạy giao diện quản lý Forefront TMG để backup hoặc khôi phục toàn bộ cấu hình TMG.

Hướng dẫn làm bài

B1: Export wizard→Next→ chỉ định mật khẩu có tối thiểu 8 ký tự để mã hóa thông tin

B2: Vị trí file lưu cần nằm trên phân vùng có định dạng NTFS→Next

B3: Import cấu hình TMG→Next→ Chỉ định location của của file cấu hình TMG đã được export→Next

B4: import →Next→ Chọn những thông tin bạn muốn import→Next

B5: Chỉ định mật khẩu được sử dụng để bảo vệ các thông tin→Next

B6: export →Firewall Policy→ URL → Forefront TMG trong Forefront TMG toolbox.

CÁC THUẬT NGỮ CHUYÊN MÔN

Các từ viết tắt	Tên đầy đủ	Ý nghĩa
AD	Active Directory	Dịch vụ thư mục
BDC	Backup Domain Controller	Sao lưu domain
DC	Domain Controller	Bộ điều khiển miền
DNS	Domain Name System	Hệ thống tên miền
IP	Internet Protocol	Giao thức Internet
OU	Oranization Unit	Đơn vị tổ chức
PDC	Primary Domain Controller	Bộ điều khiển tên miền chính
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tin
W2K3	Windows server 2003	Hệ điều hành windows server 2003
W2K8	Windows server 2008	Hệ điều hành windows server 2008
WXP	Windows XP	Hệ điều hành windows XP
Win7	Windows 7	Hệ điều hành windows7
FQDN	Full Qualified Domain Name	Tên miền đầy đủ được chứng nhận
HĐH	Hệ Điều Hành	Hệ Điều Hành
CSDL	Cơ Sở Dữ Liệu	Cơ Sở Dữ Liệu
MSDE	Microsoft Database Engine	Công nghệ cơ sở dữ liệu

RUP	Roaming User Profile	Cho phép Profile lưu trên server kèm theo user
PAP	Password Authentication Protocol	Giao thức xác nhận mật mã
CHAP	Challenge Handshake Authentication Protocol	Giao thức bảo mật dựng sẵn
EAP	Extensible Authentication Protocol	Phương thức bảo mật cho mạng không dây
DFS	Distributed File System	Hệ thống bảo mật
NAT	Network Address Translation	Biên dịch địa chỉ mạng
IPSec	Internet Protocol SECurity	Giao thức xác thực và mã hóa IP
SQL	Structured Query Language	Ngôn ngữ truy vấn
RRAS	Routing and Remote Access	Cấu hình định tuyến bằng giao diện
RDP	Remote Desktop Protocol	Tính năng truy cập máy tính trong mạng
EFS	Encrypting File System	Mã hóa dữ liệu
DFS	Distributed File System	Hệ thống tập tin phân tán
STMP	Simple Mail Transfer Protocol	Giao thức truyền thư đơn giản
SSH	Secure Shell	Dịch vụ truy cập từ xa
SSL	Secure Socket Layer	Tầng socket an toàn
RIP	Routing Information Protocol	Một kiểu giao thức dẫn đường
RARP	Reverse Address Resolution Protocol	Giao thức chuyển đổi từ địa chỉ vật lý sang địa chỉ IP
NIC	Network Interface Card	Card giao tiếp mạng
MAC	Media Access Control	Địa chỉ thiết bị

LAN	Local Area Network	Mạng nội bộ
IGMP	Internet Group Management Protocol	Giao thức Internet để các host kết nối, huỷ kết nối từ các nhóm multicast
HTTP	Hyper Text Transfer Protocol	Giao thức truyền siêu văn bản
FIB	Forwarding Information Table	Bảng thông tin chuyển đổi định tuyến
POP3	Post Office Protocol version 3	là một giao thức tầng ứng dụng, dùng để lấy thư điện tử từ server mail
NTFS	New Technology File System	Hệ thống tập tin công nghệ mới
SAM	Security Accounts Manager	Bảo mật tài khoản quản lý
SOA	Start of Authority	Thông tin về domain trên DNS Server
SID	Security Identifier	Định danh bảo mật
MMC	Microsoft Management Console	Công cụ quản lý và cấu hình windows
RR	Resource Record	Mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu DNS
FTP	File Transfer Protocol	Giao thức truyền file
URL	Uniform Resouce Locator	Địa chỉ tài nguyên thống nhất

TÀI LIỆU THAM KHẢO

- Tài liệu quản trị windows server 2003, tác giả Trung tâm tin học Đại học Khoa học Tự nhiên TPHCM, xuất bản năm 2003
- Các bài Lab MCSA, tác giả trung tâm đào tạo mạng máy tính Nhất Nghệ xuất bản năm 2005
- Tài liệu Windows Server 2003 tập 1,2,3, tác giả Phạm Hoàng Dũng do nhà xuất bản thống kê xuất bản năm 2005